EASyCAP®
Encoder/Decoder

Emergency Management System
Version 2.15
Operation Manual

think ahead.

TRILITHIC

Trilithic Company Profile

Trilithic is a privately held manufacturer founded in 1986 as an engineering and assembly company that builds and designs customer-directed products for telecommunications, military, and industrial customers. From its modest beginnings as a two-man engineering team, Trilithic has grown over the years and broadened its offerings of RF and microwave components by adding broadband solutions to its product line. This was accomplished with the acquisition of components manufacturer Cir-Q-Tel and instruments manufacturer Texscan.

Today, Trilithic is an industry leader, providing telecommunications solutions for major broadband, RF and microwave markets around the world. As an ISO 9000:2001 certified company with over 40 years of collective expertise in engineering and custom assembly, Trilithic is dedicated to providing quality products, services and communications solutions that exceed customer expectations.

Trilithic is comprised of five major divisions:

- **Broadband Instruments and Systems**
  Offers test, analysis, and quality management solutions for the major cable television systems worldwide.
- **RF Microwave Components**
  Provides components and custom subsystems for companies specializing in cellular, military, and other wireless applications.
- **Emergency Alert Systems**
  Leading supplier of government-mandated emergency alert systems used by broadcast TV, cable TV, IPTV, DBS, and radio stations.
- **XFTP**
  Offers a specialty line of field technical products for cable operators and technicians, as well as a line of products for installing electronics in the home of the future.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

General Information 5
Introduction 5
FCC Certification 6
Unpacking and Inspection 6
Claims for Damage in Shipment 6
Helpful Website 7
Where to Get Technical Support 7
How this Manual is Organized 8
Conventions Used in this Manual 8
Security Recommendations 9
Overview 10
Wiring Recommendations 10
Hardware Overview 11
Front Panel View 11
Rear Panel View 12
Front Panel Menu Overview 21
Touch Screen LCD 21
Main Screen (Home Page) 21
Alert Playback Screen 23
Login Menu 23
Setup Menu 24
Network Setup Menu 24
Ethernet Interface Setup Menu 25
IP Address Entry Menu 25
System Menu 26
Front Panel Menu 26
Configuration 28
System Login 28
EASyCAP® User Interface Homepage 29
Administration Folder 31
Account Preferences 31
User Accounts 32
Backup/Restore Configuration 35
Licensing 35
Upgrade 36
Reboot 37
Configuration Folder 38
Audio/Tone Volume 38
Audio/Radios Sources 41
Date/Time 43

EAS Events....44
EAS Options....46
MPEG Stream....48
Network Configuration....50
Playback Options....55
Selected Locations....57
Selected States....58
Video Out....59
Web Configuration....60
CAP Sources....61
CAP Proxy Configuration....61
Campus Alert Feed....62
ComLabs EMnet Client....63
EASyPLUS EAS-CAP Feed....65
IPAWS Atom Feed....66
MyStateUSA Feed....67
TCP Feed....68
Message Delivery Folder....69
Atom CAP Server....69
CAP HTTP Delivery....71
EASyPLUS....75
DCM....76
DNCS/Evertz....77
IP Switches....79
Minerva Configuration....80
SCTE-18 Configuration....81
Serial Devices....86
Management Folder....87
Email....87
SNMP....89
SYSLOG....91
Web API....92
Logs....93
Alert/ System Log....93
Operations....95
Alert Status Monitor....95
Custom Messaging....98
Generate EAS....99
Appendix....101
Telephone Interface....101
Specifications....108
Trilithic EAS 2-Year Limited Warranty....110

Chapter 1
General Information

Introduction

The Trilithic EASyCAP® (Model EASyCAP-1) EAS (Emergency Alert System) Encoder/Decoder is a 2U rack mounted control center capable of performing manual or automated EAS messaging for Cable, Broadcast, IPTV, and Wire line systems and is in accordance with CFR 47 part 11 FCC regulations.

The EASyCAP® Encoder/Decoder receives EAS messages from up to six audio sources (internal or external), decodes the FSK EAS message, and operates the target system equipment to replay the message for viewers/listeners. In addition, messages can be originated by the user via local or remote control of the EASyCAP®. The EAS Audio sources for the EASyCAP® include internal AM/FM/NOAA radios and external audio inputs that can be connected to any known EAS audio source. EAS Audio is decoded by the internal AFSK circuitry, then sorted and interpreted to determine the type of emergency or test, locations for which the emergency applies, and other information supplied in the EAS Header. If a voice message is contained in the EAS message, it is recorded for possible playback to subscribers. EAS messages then pass through a series of tests to determine if the message matches predefined, user configurable parameters. If these tests pass, EAS activation (message playback) to the system occurs. To play an EAS message to viewers/listeners, the EASyCAP® activates TTLs, Contact Closures, RS-485 data commands, RS-232 data commands, and several IP based protocols, it also supplies pertinent video and re-encodes/plays the EAS FSK and recorded audio. The TTLs, Contact Closures, and serial data commands, and IP protocols activate routing equipment and end-user devices to provide the emergency audio and video to all viewers/listeners.

In addition to the EAS messaging capabilities, the EASyCAP® records all received and transmitted messages in the internal log for later retrieval.

FCC Certification

The Trilithic EASyCAP® Encoder/Decoder is certified to comply with 47 CFR, Part 11 (FCC regulations) for EAS encoders and decoders, and is registered with the FCC under identification number: P4V-EASYCAP-1.

Pursuant to FCC 15.21 of the FCC rules, changes not expressly approved by Trilithic, Inc. might cause harmful interference and void the FCC authorization to operate this product.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an output on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Unpacking and Inspection

When the EASyCAP® Encoder/Decoder arrives, immediately inspect the shipping container and contents for visible damage. Keep all packing materials until the equipment's intended performance characteristics have been verified. If any of the equipment is damaged or fails to operate properly due to transportation damage, immediately file a claim with the transportation company or, if insured separately, with the insurance company.

Each EASyCAP® Encoder/Decoder will arrive in its own shipping container. The container will, at a minimum, include the following components; EASyCAP® Encoder/Decoder and AC Power Cord.

Claims for Damage in Shipment

Claims for shipping damage should be directed to the shipping and/or freight delivery service. Claims should be made within 7 days to insure prompt handling of the claim.

Helpful Website

The following website contains general information which may be of interest:

http://www.trilithic.com

Trilithic's website contains product specifications and information, tips, release information, product updates, marketing information, Frequently Asked Questions (FAQs), bulletins, and other technical information.

Where to Get Technical Support

Trilithic technical support is available Monday through Friday from 8:00AM to 5:00PM EST. Callers in North America can dial 1-317-895-3600 or 1-800-344-2412 (toll free). International callers should dial 1-317-895-3600 or fax questions to 1-317-895-3613. You can also e-mail technical support at EASysupport@trilithic.com.

For quicker support response when calling or sending e-mail, please provide the following information:

- Your name and your company name
- The technical point of contact (name, phone number, e-mail)
- The serial number of the EASyCAP® Encoder/Decoder
- A detailed description of the problem you are experiencing, including any error or information messages

Before any Trilithic EAS Encoder/Decoder can be returned for repair, Trilithic will issue a return material authorization (RMA) number. NO RETURNED EQUIPMENT WILL BE ACCEPTED WHICH DOES NOT HAVE AN RMA NUMBER PROMINENTLY DISPLAYED ON THE OUTSIDE SHIPPING CARTON AND ON THE SHIPPING LABEL. A complete and full description, in writing, regarding the service issues with the equipment must be supplied inside the shipping container with each piece of equipment for which an RMA number has been issued.

NOTE

Hardware or software modifications and changes may occur at any time during production, shipping, and/or during the equipment's life span. These changes may occur or be implemented by Trilithic, Inc. without prior written notice or warning.

How this Manual is Organized

This manual is divided into the following chapters:

- Chapter 1, “General Information,” provides Trilithic contact information and describes how this operation manual is structured.
- Chapter 2, “Overview” gives an overview of the EASyCAP® Encoder/Decoder hardware and how it works.
- Chapter 3, “Configuration” describes the steps necessary to configure the EASyCAP® Encoder/Decoder.
- Chapter 3, “Appendix” describes the specifications and warranty of the EASyCAP® Encoder/Decoder.

Conventions Used in this Manual

This manual has several standard conventions for presenting information.

- Connections, menus, menu options, and user entered text and commands appear in **bold**.
- Section names, web, and e-mail addresses appear in *italics*.

NOTE

A NOTE is information that will be of assistance to you related to the current step or procedure.

CAUTION

A CAUTION alerts you to any condition that could cause a mechanical failure or potential loss of data.

WARNING

A WARNING alerts you to any condition that could cause personal injury.

Security Recommendations

Where possible, EAS Participants should adhere to the security best practices recommendation for EAS participants contained in the Communications Security, Reliability and Interoperability Council (CSRIC) EAS Security Subcommittee report.

EASyCAP® Software/Firmware upgrades are available at http://eas.trilithic.com/Documents/Firmware/index.html or by sending inquiries to easysupport@trilithic.com. Trilithic recommends checking for upgrades at least every six months. If you become aware of security vulnerabilities for the Debian Linux operating system you should check for Trilithic EASyCAP® upgrades.

EASyCAP® upgrades are performed using the Web GUI by accessing the Administration/ Upgrade screen, which provides a means to upload and install the upgrade file. If the upgrade file has a .zip file extension it will also contain a readme text document providing important information or special instructions for the upgrade.

While EASyCAP® Encoder/Decoders utilize an internal firewall, Trilithic strongly recommends the use of an external router and firewall for connections facing the internet. Alternatively an http proxy may be used. A three-tier architecture is recommended.

- If able to manage the EASyCAP® from an internal private network (LAN), the internet facing firewall should completely block incoming connections while allowing outbound connections on port 443.
- If management over the internet is required, use of Network Address Translation to port 443 for the Web GUI is highly recommended. The internet exposed port should be a non-standard port (not a well-known port) between 11000 and 65000, and should avoid ending in common port numbers such as 21, 22, 80, and 443.
  - Some web browsers or other security features will not allow https connections over a port other than 443. In such a configuration there is no choice but to use port 443 for incoming connections.
  - If possible, restrict incoming IP addresses to known address ranges for your organization.
- If there is no choice but to place the EASyCAP® directly on the Internet
  - The non-secure web server interface should be disabled. Turn on the option to use secure https access in the Configuration/Web Configuration settings.
  - Disable the “Allow SSH” checkbox in the network settings for the internet-facing interface.
  - If the web interface is not required for the internet-facing connection, disable the “Allow Web Server” checkbox in the network settings for the internet-facing interface.
- Where possible, the Internet facing Ethernet port should be avoided for management and system activation protocols.

Wiring Recommendations

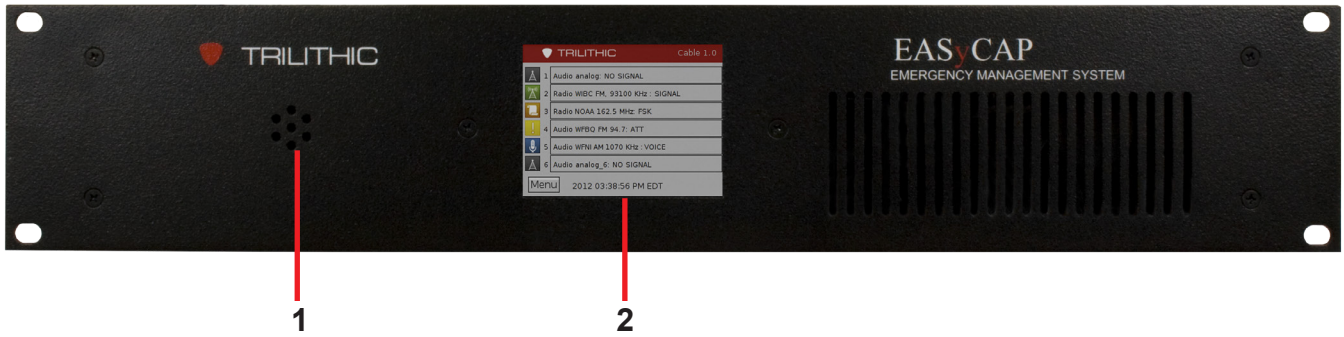
- Shielded audio wire for all TTL, contact closure, and audio connections
- Shielded RS-232 cable
- Shielded (coaxial) video cables
- Shielded Category 6 or 7 Ethernet cables for all Ethernet connections

CAUTION

The EASyCAP® Encoder/ Decoder should be installed in a rack that is properly grounded.

Hardware Overview

Front Panel View

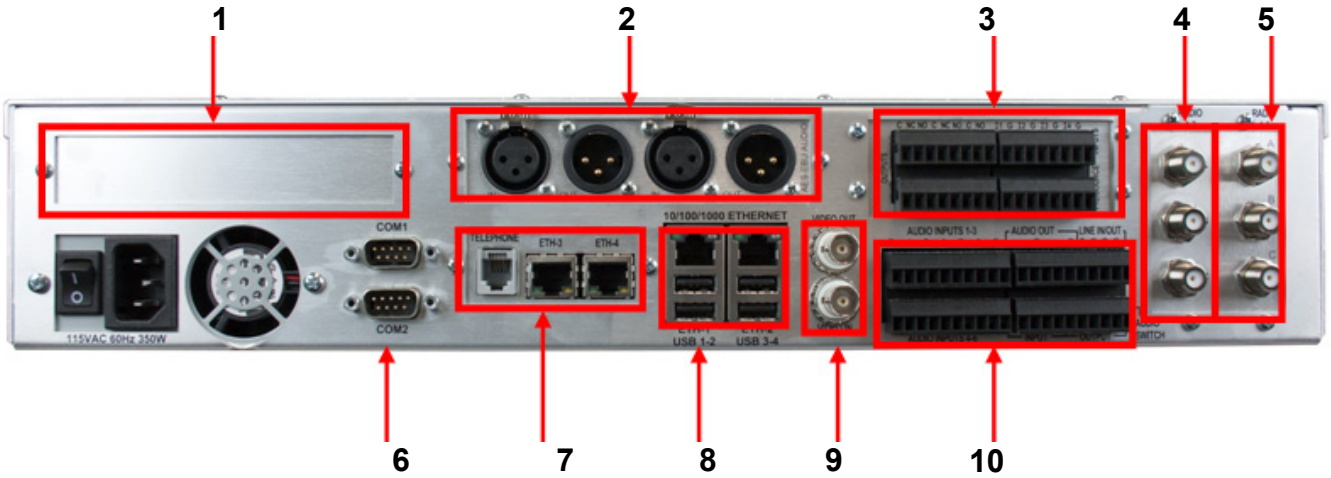


1. **Speaker** - Used for monitoring audio inputs and to provide aural feedback during EAS activations.
2. **Touchscreen LCD Display** - Provides visual feedback during programming, setup, monitoring, and activations and it is used for local control of the EASyCAP® and access to the on-board menu system.

NOTE

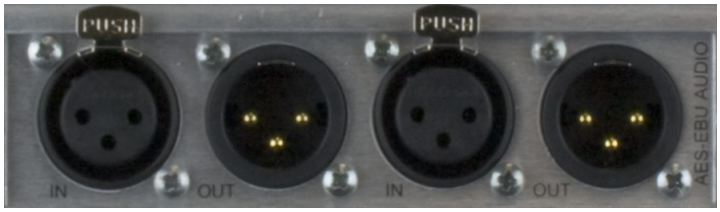
The keypad and LCD display provide an on-board menu system, allowing for a limited amount of configuration, tests, and encoding functions. A secure web interface provides more comprehensive configuration and control of the encoder/decoder.

Rear Panel View



1. **PCIe Expansion Slot (Optional)** - This is a PCI Express expansion slot that will accommodate a 1, 4, or 16 lane PCIe card. This is reserved for future use. Only use cards approved by Trilithic. Use of unapproved cards may void warranties and render the equipment inoperable, and cannot be supported by Customer Support.

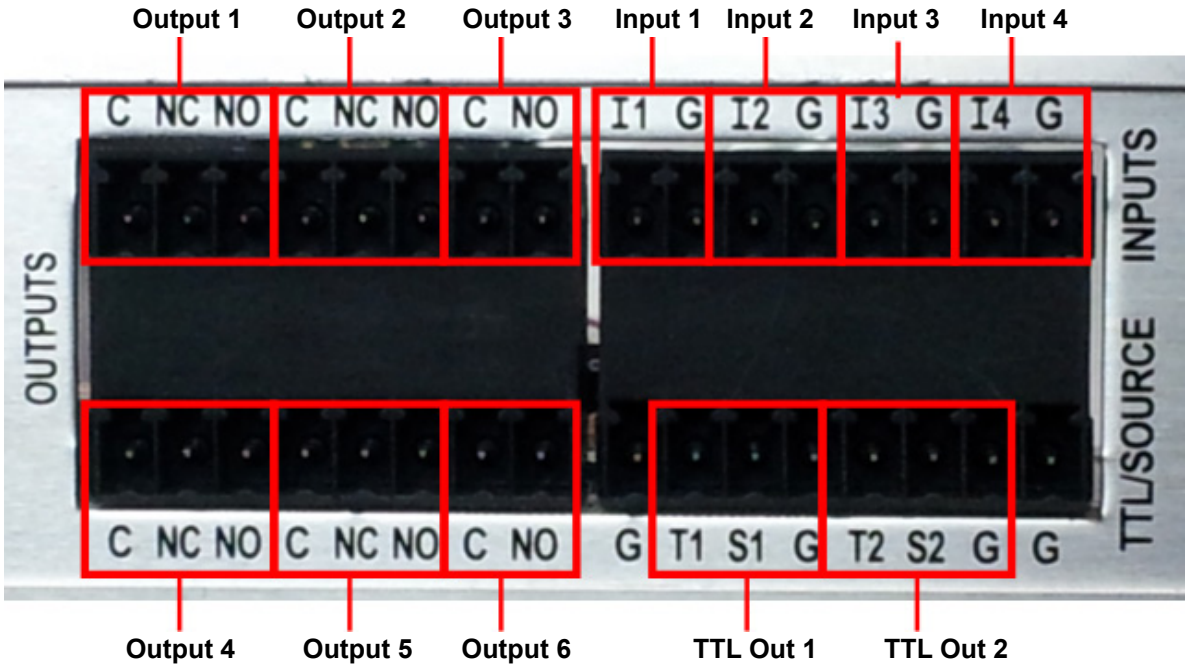
2. **Audio Expansion Slot (Optional)** - One slot is provided for expansion audio boards. An AES-EBU digital audio board is currently available. Additional cards may be available. Contact EAS Customer Support for information.



AES-EBU Digital Audio Board - Provides independent synchronized AES-EBU audio switches for in-line replacement of programming audio during EAS operations. It includes two (2) AES-EBU digital audio switches on 110 Ohm XLR connections. The internal switches replace the normal AES-EBU program audio with alert audio. The alert audio automatically locks to the incoming bit rate and sample rate (up to 192 kHz). If no input is provided, the output sample rate will be 48KHz. Bypass relays are provided to ensure the program audio is not interrupted during a power loss.

AES-EBU Input 110 Ohm XLR female	**AES-EBU Output - 110 Ohm XLR male**
Pin 1: Ground/drain	**Pin 1:** Ground/drain
Pin 2: Balanced +	**Pin 2:** Balanced +
Pin 3: Balanced -	**Pin 3:** Balanced –

3. **General Purpose Inputs/Outputs** - The EASyCAP® Encoder/Decoder comes standard with six (6) general purpose outputs, four (4) general purpose inputs, and two (2) TTL outputs. Additional cards may be available, contact EAS Customer Support for information.



General Purpose Outputs – Six (6) contact closure outputs (switches) are provided for activating equipment to route the alert audio and video, sound alarms, and activate other devices during EAS transmission. When an output is active, the common and normally opened terminals are shorted together (closed).

(C) Common contact

(NC) Normally-closed contact

(NO) Normally-open contact

Broadcast

Output 1, Transmitting Audio – Activates when alert audio playback is in progress. This is used to activate audio distribution and routing equipment during EAS activations in order to replace the normal program audio with the alert audio.

Output 2, Transmitting – Activates when alert playback is in progress (audio and video). This is used to activate audio and video distribution and routing equipment during EAS activations in order to replace the normal program audio and video with the alert information.

Output 3, Transmitting – Activates when alert playback is in progress (audio and video).

Output 4, Alert Ready – Activates when an alert has been received and is waiting for operator confirmation before being transmitted.

Output 5, EAN Active – Activates when an EAN (Emergency Action Notification) is in progress.

Output 6, Reserved – This output is reserved for future use.

Cable TV and IPTV

Output 1, Transmitting Audio – Activates when alert audio playback is in progress. This is used to activate audio distribution and routing equipment during EAS activations in order to replace the normal program audio with the alert audio.

Output 2, Transmitting – Activates when alert playback is in progress (audio and video). This is used to activate audio and video distribution and routing equipment during EAS activations in order to replace the normal program audio and video with the alert information.

Output 3, Transmitting – Activates when alert playback is in progress (audio and video).

Output 4, Time Adjusted – Activates a configurable number of seconds before or after the alert audio and video playback begins and deactivates a configurable number of seconds before or after the alert playback ends. It is used to trigger equipment that requires time to acquire the EAS audio/video, create an MPEG stream, or send commands across a network.

Output 5, EAN Active – Activates when an EAN (Emergency Action Notification) is in progress.

Output 6, Reserved – This output is reserved for future use.

TTL Outputs - These outputs provide a five (5) volt DC signal (and ground connection) used to activate EAS audio and video routing equipment. A current source is also provided.

Broadcast

TTL 1, Transmitting Audio – Activates anytime alert audio playback is in progress.

TTL 2, Transmitting – Activates anytime alert playback is in progress (audio and video).

Cable TV and IPTV

TTL 1, Transmitting – Activates anytime alert playback is in progress (audio and video).

TTL 2, Reserved – This output is reserved for future use.

General Purpose Inputs – Four (4) general purpose inputs provide a means for operators and external automation equipment to trigger and abort EAS activations.

Input 1, Abort – When closed (shorted), stops playback of the EAS message in progress. The EASyCAP® will attempt to stop all video and audio replacement equipment and then return to monitoring for incoming alert messages. This input is edge-triggered. Holding it closed will not continuously abort messages.

(G) Contact ground

(I1) Opto-isolated input

Input 2, Trigger Pending Message– This input is only used when the EASyCAP® is in manual mode. When an alert message is ready for transmission, it will wait for user confirmation. When this input is closed (shorted), it causes the pending EAS message to begin transmission, regardless of the state of the hold-off input (input 3). This input is edge-triggered. Holding it closed will not continuously trigger messages.

(G) Contact ground

(I2) Opto-isolated input

Input 3, Hold-off Pending Message– This input is only used when the EASyCAP® is in manual mode. It is normally used by automation equipment to hold off alert message playback. When closed (shorted), this input will prohibit pending EAS messages from transmitting. When the input is opened, pending EAS messages will begin transmission.

(G) Contact ground

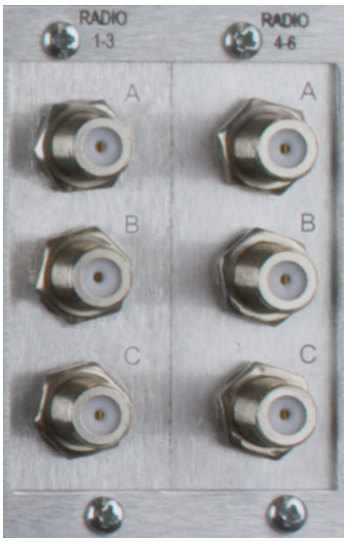
(I3) Opto-isolated input

Input 4, Generate RWT–When this input is momentarily closed, a Required Weekly Test will be generated. This input is edge-triggered. Holding it closed will not continuously generate Required Weekly Tests.

(G) Contact ground

(I4) Opto-isolated input

4. **Radios 1-3 (optional)** - A radio receiver board with three (3) AM/FM/NOAA radio receivers can be installed. Each radio receiver can be independently tuned to AM, FM, or NOAA and includes a nominal 75 ohm antenna input. The radios are provided to monitor EAS sources. Each audio input can be configured as an internal radio receiver or audio from an external source (using the analog audio inputs).



   (A) Channel 1 radio receiver antenna input (75 ohm F connector)

   (B) Channel 2 radio receiver antenna input (75 ohm F connector)

   (C) Channel 3 radio receiver antenna input (75 ohm F connector)

5. **Radios 4-6 (optional)**– A radio receiver board with three (3) AM/FM/NOAA radio receivers can be installed in this slot, providing up to 6 internal radio receivers. Each radio receiver can be independently tuned to AM, FM, or NOAA and includes a nominal 75 ohm antenna input. The radios are provided to monitor EAS sources. Each audio input can be configured as an internal radio receiver or audio from an external source (using the analog audio inputs).

   (A) Channel 4 radio receiver antenna input (75 ohm F connector)

   (B) Channel 5 radio receiver antenna input (75 ohm F connector)

   (C) Channel 6 radio receiver antenna input (75 ohm F connector)

6. **RS-232 Serial Ports** – Two (2) RS-232C compliant serial data connections are provided on DB-9 male connectors.

COM-1 (top DB-9 connector) – This port provides a command line console into the EASyCAP® for low-level configuration, control, and troubleshooting.

COM-2 (bottom DB-9 connector) – This port can be configured to provide EAS information to external equipment such as character generators, sign boards, and logging/monitoring systems.

9-pin RS-232C DTE Interface – Normally connects to PCs or equipment with a 9-pin NULL-MODEM cable.

Pin 2: Receive data*	**Pin 3:** Transmit data*
Pin 4: Data terminal ready	**Pin 5:** Signal ground*
Pin 6: Data set ready	**Pin 7:** Request to send
Pin 8: Clear to send	**Pin 9:** Ring indicator

* Required signal

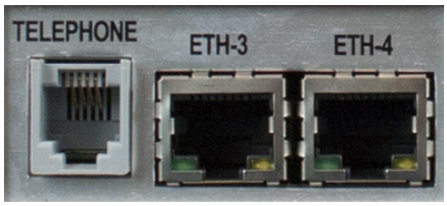
7. **Communications Expansion Slot** – The EASyCAP® can accommodate one (1) optional communications expansion board. There are currently two communication expansion boards available. Additional cards may be available. Contact EAS Customer Support for information.

Expansion communications board with LAN/MODEM/RS-485

- One (1) 10/100 Ethernet Port
- One (1) Telephone Modem Port (56K data and voice) – allows DTMF and data communication for remote control of the EASyCAP®, and remote generation of emergency messages.
- One (1) half-duplex RS-485 Port - 1/8th load RS-485 communications port provided for controlling external character generators.

Expansion communications board with Dual LAN and MODEM

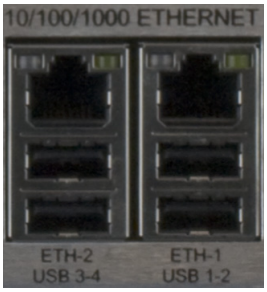
- Two (2) 10/100 Ethernet Ports
- One (1) Telephone Modem Port (56K data and voice) – allows DTMF and data communication for remote control of the EASyCAP®, and remote generation of emergency messages.



8. **Ethernet and USB Ports**

Ethernet – Two (2) 10/100/1000 Ethernet ports provide an interface for remote management of the EASyCAP®, monitoring CAP feeds, and providing EAS information to downstream audio, video, and distribution equipment.

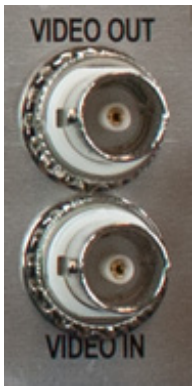
USB Ports – Four (4) USB ports are provided. Only use devices approved by Trilithic. Use of unapproved devices may void warranties and render the equipment inoperable, and cannot be supported by Customer Support.



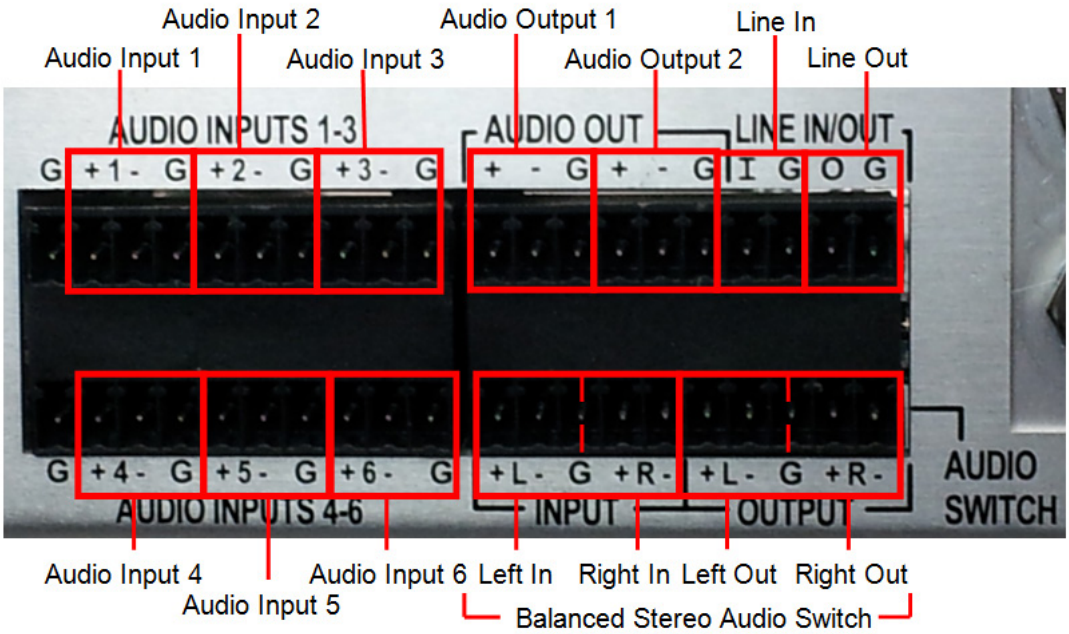
9. **CG VIDEO-**The EASyCAP® includes an internal analog video character generator to display the alert text. An internal analog video switch is provided to automatically switch the internal character generator into the program video during message playback. It includes a video bypass relay to ensure that the program video is not interrupted during a power loss.

VIDEO IN – NTSC video input connection to the internal video switch for the normal program video.

VIDEO OUT – NTSC video output connection from the internal switch. The video output normally contains the program video fed into the input. During alert message playback, the output is automatically switched to the internal character generator.



10. Audio Inputs and Outputs



Audio inputs – Six (6) balanced 600 ohm audio inputs are provided to monitor external audio sources for EAS. They can be connected to audio sources such as external radio receivers, TV tuners, and satellite receivers. Configuration is provided to select between external audio sources and internal radio receivers for each input.

- **(+)** Positive analog audio input for the respective channel
- **(-)** Negative analog audio input for the respective channel
- **(G)** Ground

Audio outputs – Two (2) balanced 600 ohm audio outputs are provided for the alert audio. They can be connected to EAS distribution and routing equipment. The outputs contain audio generated by the EASyCAP® during EAS activations.

- **(+)** Positive analog audio output
- **(-)** Negative analog audio output
- **(G)** Ground

Line Input – A line-level mono audio input is provided to record audio. This can be connected to a line-level microphone or audio source (such as a computer sound card) in order to record audio for message origination.

(I) Positive analog audio input

(G) Ground

Line Output – A line-level audio output is provided to monitor the EASyCAP® audio on external speakers. It contains the same audio as the front panel speaker and can be used to monitor the EASyCAP®.

(O) Positive analog audio output

(G) Ground

Audio Switch – A 600 ohm balanced stereo audio switch is provided to replace normal program audio with alert audio during EAS activations. The switch includes a bypass relay to ensure that program audio is not interrupted during a power loss.

Input – Connect normal program audio to the audio switch input.

Output – Connect the audio switch output into the normal program audio path. The output from the audio switch normally contains the program audio fed into the input. During EAS activations, the output contains the alert audio.

Audio Switch Terminals (from left to right)

Inputs

(-) Negative analog audio input for the left channel

(+) Positive analog audio input for the left channel

(G) Ground

(-) Negative analog audio input for the right channel

(+) Positive analog audio input for the right channel

Outputs

(-) Negative analog audio output for the left channel

(+) Positive analog audio output for the left channel

(G) Ground

(-) Negative analog audio output for the right channel

(+) Positive analog audio output for the right channel

Front Panel Menu Overview

Touch Screen LCD

The EASyCAP® Encoder/Decoder includes a touch-screen LCD on the front panel to provide EAS status indicators and a simple graphical user interface for a limited amount of configuration and control.

Main Screen (Home Page)

The Main screen is displayed when the system is idle and monitoring for EAS messages. The EASyCAP® application type and software version are displayed in the top right corner of the screen. The bottom line shows the current date and time of the EASyCAP®.

The **Menu** button is located in the bottom left corner of the screen to allow access to the front panel menu.

Current Status

The current status of each EAS audio input is displayed on the main screen. The following information is displayed for each audio input:

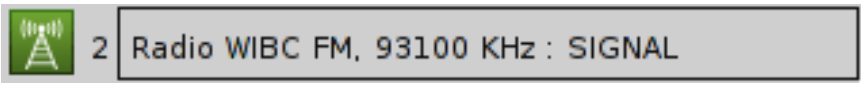
- Channel
- Type of audio source – “Audio” if the input is configured to receive audio from an external audio source or “Radio” if the input is configured as an internal radio.
- Configured name of the audio source
- The current status
- If the input is an internal radio - the radio station frequency is displayed.

Status: NO SIGNAL

A status of “NO SIGNAL” indicates that audio is not detected at this input.

Status: SIGNAL

A status of “SIGNAL” indicates that audio is detected at this input.

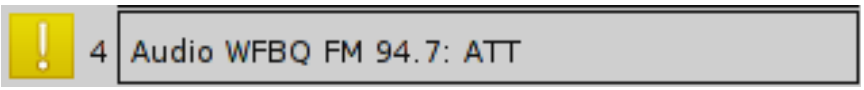


Status: FSK

A status of “FSK” indicates that EAS FSK is being received on this input.

Status: ATT

A status of “ATT” indicates that an Attention Tone is being received on this input.



Status: VOICE

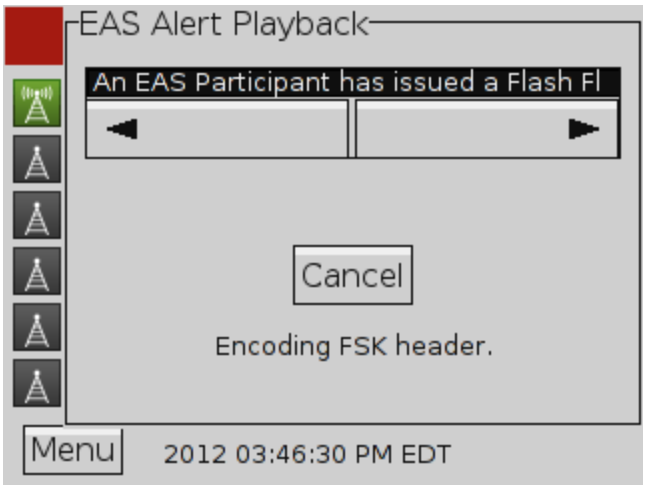
A status of “VOICE” indicates that an EAS Voice Message is being recorded.

Alert Playback Screen

The **EAS Alert Playback** screen is displayed during EAS message playback. The alert text of the current alert playback can be viewed.

Select the **Cancel** button to stop the current message playback. It will end the local playback and, where possible, send cancel messages to configured external equipment.

When running a Broadcast Application in manual mode a Confirm button will be displayed on this screen to allow the operator to confirm that the alert should be transmitted.

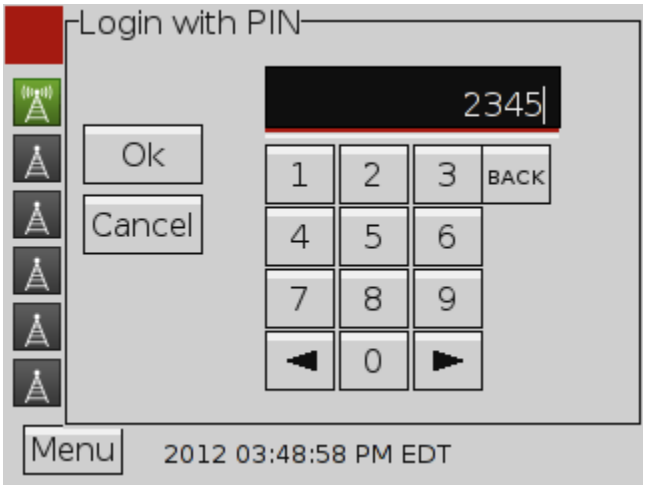


Login Menu

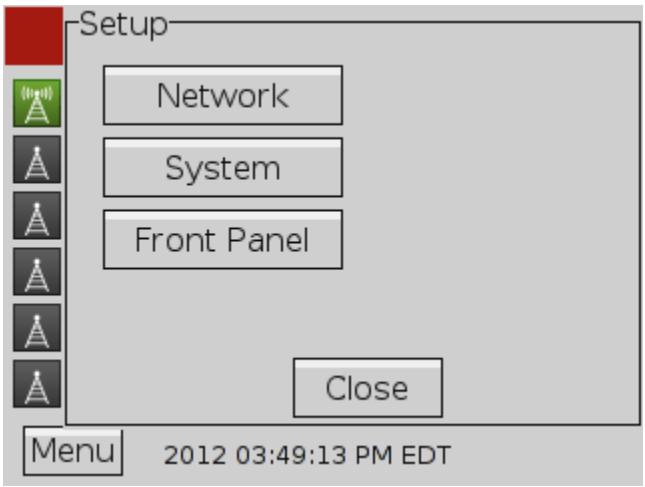
The **Login** screen is displayed after the **Menu** button is selected. A valid User PIN must be entered before entering the menu. Note that the user account must have configuration privileges.

Enter your User PIN (4-8 digit code) and select the **OK** button. The factory default PIN is 2345.

To go back to the **Main** screen and cancel the Login, select the **Cancel** button.



Setup Menu



The **Setup** screen is displayed after logging into the menu. It provides access to any available menus for configuration and control.

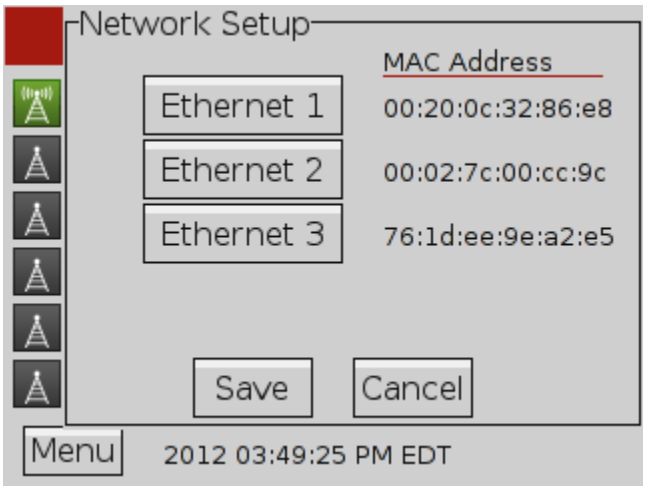
Network button – Displays the **Network Setup** menu. This menu allows you to view and change network settings.

System button – Displays the **System Control** menu. This menu allows you to restart the EASyCAP®, and to encode a RWT.

Front Panel button – Displays the **Front Panel Configuration** menu. This menu allows you to configure the themes (colors and styles) for the LCD and on-board menu.

Close button – Exits the **Setup** menu and returns to the **Main** screen.

Network Setup Menu



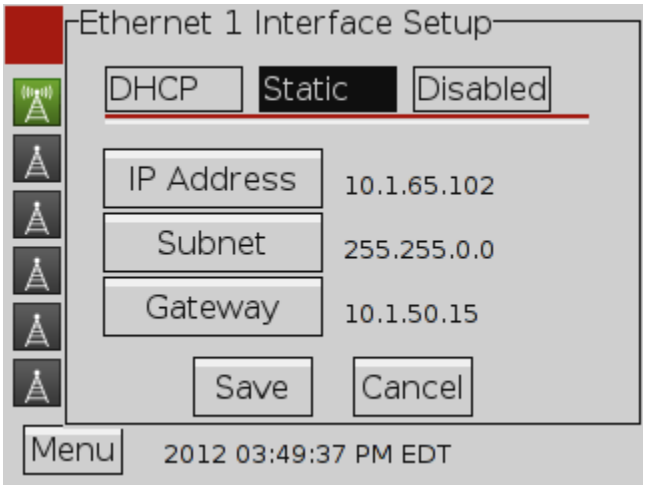
The **Network Setup** menu displays the available network interfaces and the MAC address of each. A button is provided to view and change the settings for each network interface.

Ethernet <N> button – Opens the configuration menu for the selected network interface.

Save button – Saves any changes made to the network interfaces settings and closes the **Network Setup** menu.

Cancel button – Cancels any changes made to the network interfaces settings and closes the **Network Setup** menu.

Ethernet Interface Setup Menu



The **Ethernet Interface Setup** menu shows the current settings for the interface and provides controls to change the interfaces settings.

DHCP/Static/Disabled – Select if the Ethernet interface is configured automatically using DHCP or manually using Static configuration. The interface can also be disabled.

When DHCP is selected, all network settings are obtained automatically from the DHCP server. No additional settings are needed.

IP Address button – Displays a menu with a keyboard to enter the Static IP Address.

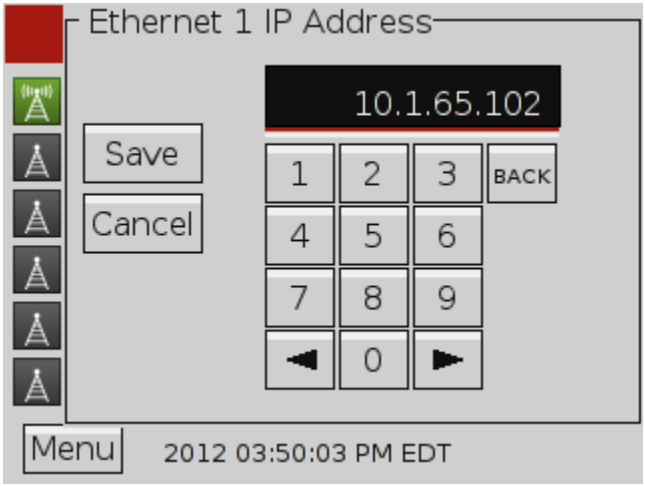
Subnet button – Displays a menu with a keyboard to enter the interfaces subnet mask.

Gateway – Displays a menu with a keyboard to enter the IP address for the Default Gateway.

NOTE

When network settings are saved from the front panel menu, SSH and the Web Interface will be enabled for all interfaces.

IP Address Entry Menu



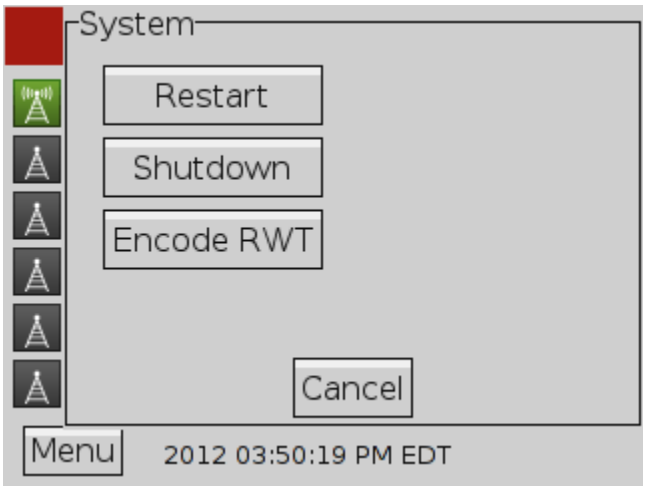
The **Ethernet IP Address** menu provides an edit box and keyboard to allow IP addresses to be entered. Enter the IP address using the keypad. This menu is also used to enter a subnet mask and gateway address.

Select the **Save** button to save the IP address.

Press the **Cancel** button to discard changes to the IP address and close the **Ethernet IP Address** menu.

System Menu

The **System** menu provides controls to restart and shutdown the EASyCAP® unit. Operators can also generate RWT messages from this menu.



Restart – Restarts (reboots) the EASyCAP® unit.

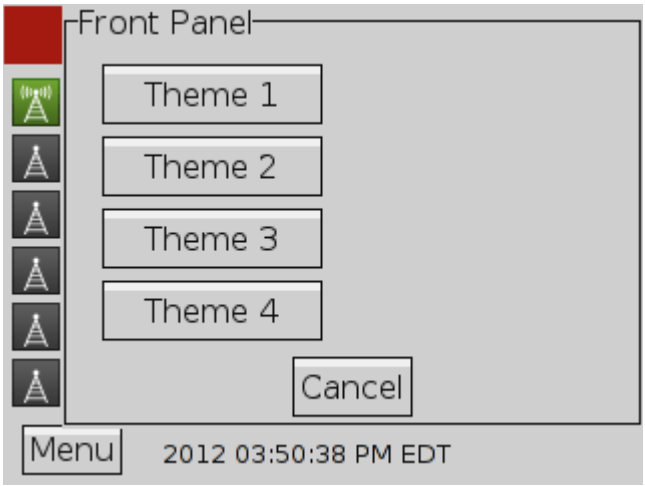
Shutdown – Shuts down the EASyCAP® unit. Turn the power switch off after the system has completed shutdown (power is not automatically removed).

Encode RWT – Generates a RWT message. FIPS codes for the RWT are configured through the Web Interface (EAS Options).

Cancel – Closes the **System** menu.

Front Panel Menu

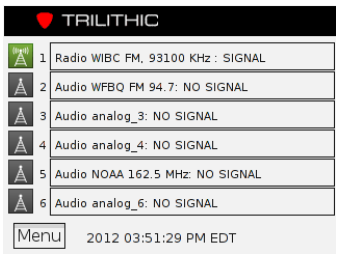
The **Front Panel** menu allows some customization of the colors and styles used for the LCD and on-board menu. Select from four themes.

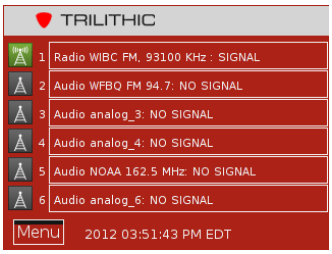


Theme <N> – Select the theme for the LCD and menu (see sample of themes below).

Cancel – Closes the **Front Panel** menu.

Available Themes





THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 3
Configuration

System Login

A web server is provided to manage the EASyCAP® Encoder/Decoder. The web interface can be configured to use HTTP on port 80 and HTTPS (secure) on port 443. The EASyCAP® is shipped from the factory with both secure (HTTPS) and non-secure (HTTP) interfaces enabled. Trilithic recommends using Chrome or Firefox web browsers.

The following should be noted when using the secure web server:

- The certificate shipped with the EASyCAP® Encoder/Decoder is not signed by a trusted certificate authority, so web browsers will display a security alert about the certificate when connecting for the first time. At this point, acknowledge the security alert and continue to the site even though the certificate isn't trusted.
- When using Mozilla Firefox, the web browser will retain the security setting for the next time you connect the server. If you are using Chrome or Internet Explorer, the security alert will be displayed every time that you connect to the web server. To disable the security alert, install a trusted certificate for the web server from the Web Configuration screen or install the EASyCAP® certificate on your PC. To install the EASyCAP® certificate on your PC from Internet Explorer, click on the **Certificate Error** message (next to the URL), click **View Certificates**, then click **Install Certificates**.

Perform the following steps to login to the EASyCAP® Encoder/Decoder:

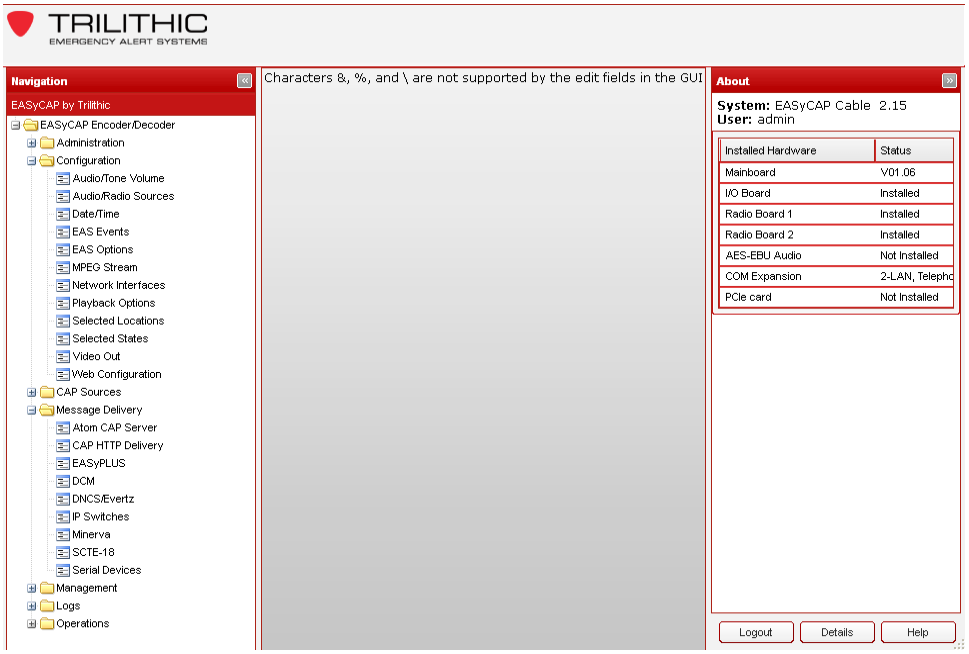
1. Enter http:// followed by the IP address of the EASyCAP® Encoder/Decoder into the URL bar of the web browser and then press **Enter** on your keyboard. Enter https:// followed by the EASyCAP® address to login to the secure web server on port 443.
2. The **EASyCAP® Login** screen will appear. Enter the username and password for the desired user account and then press the **LOGIN** button. The factory default user account has a username and password of ***Administrator***.

CAUTION

If an error message appears warning you to change your password, open the Administration/User Accounts screen and change your account password.

EASyCAP® User Interface Homepage

After logging into the system, the homepage will be displayed as shown below.



The following items can be viewed from the homepage:

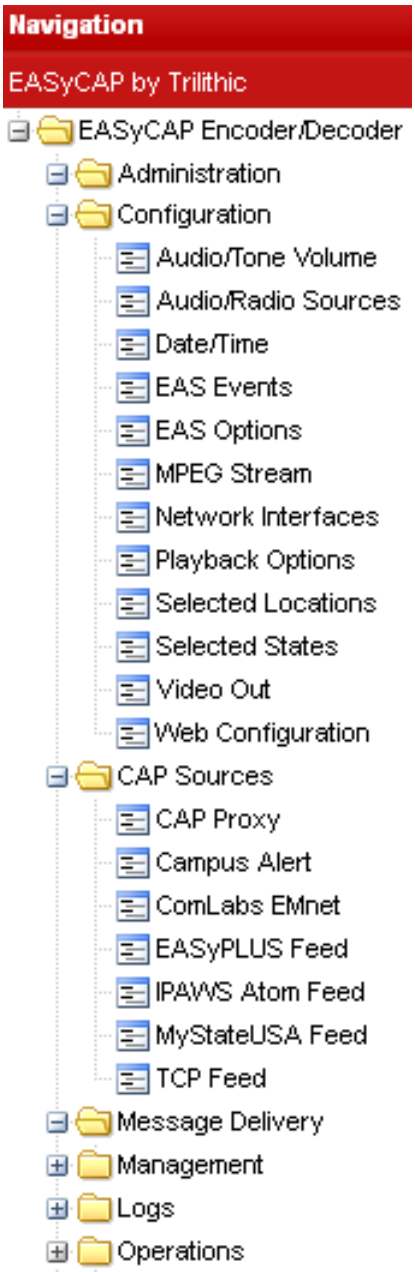
About – This area on the right side of the homepage shows the EASyCAP® Encoder/ Decoder software version, installed hardware, and current login user name.

Logout – Click this button to logout of the system.

Details – Displays information about the EASyCAP® Encoder/Decoder, including installed hardware, system information, and network information.

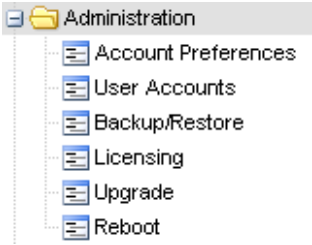
Help – Displays the EASyCAP® Encoder/Decoder Operation Manual.

Navigation – The bar on the left hand side of the homepage is used to navigate to each of the pages. The pages are sorted into folders/categories according to function; **Administration**, **Configuration**, **CAP Sources**, **Message Delivery**, **Management**, **Logs,** and **Operations**. Select the plus (+) sign to expand a category and select the minus (-) sign to collapse a category. To view a page, select the corresponding link inside each folder.



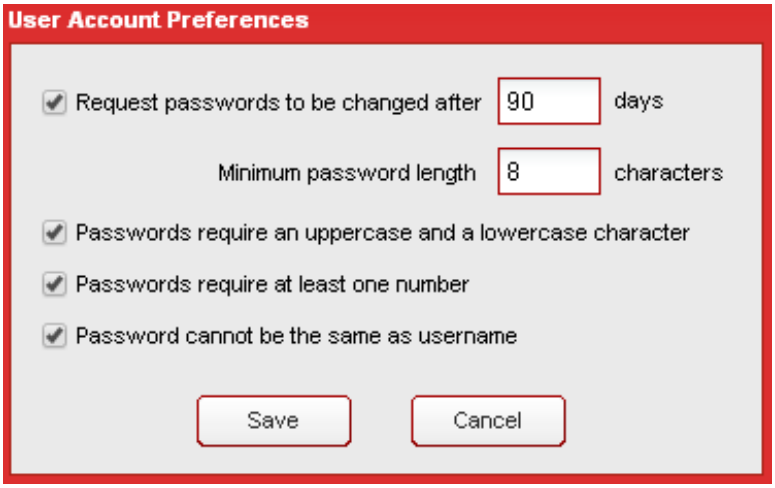
Administration Folder

In the Navigation bar, click the **+** sign next to the Administration folder to expand the folder.



Account Preferences

To setup the user account preferences for the EASyCAP®, click **Account Preferences** in the Administration folder. The account preferences are used to customize password aging and complexity. To comply with recommendations from the CSRIC EAS Security Best Practices, users should be required to change their passwords periodically, and weak passwords should be prevented.



Request passwords to be changed after xx days – When enabled, users will be prompted to change their password after a configurable number of days (30 - 365) and a warning will appear every time a user logs in with an expired password.

Minimum password length – Enter the minimum number of characters allowed for passwords (4 - 32).

Passwords require an uppercase and lowercase character – When enabled, all passwords must include at least one uppercase character and at least one lowercase character.

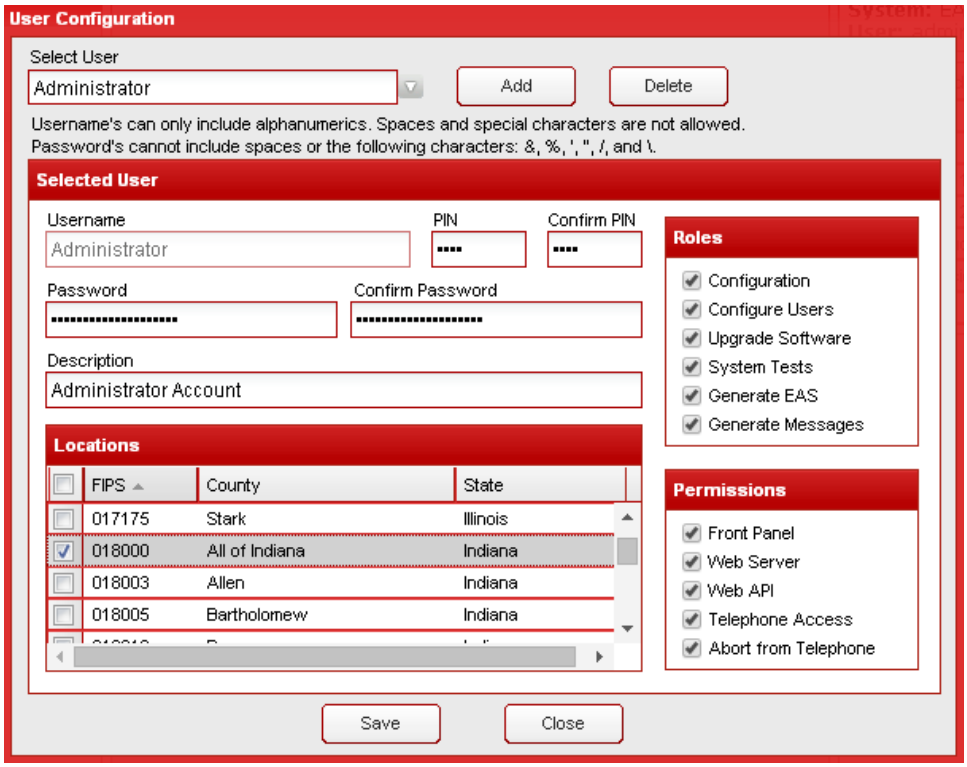
Passwords require at least one number – When enabled, passwords must include at least one number (0 - 9).

Passwords cannot be the same as username – When enabled, passwords are not allowed to be the same as the username.

Select the **Save** button to save configuration changes or **Cancel** to exit without saving.

User Accounts

To setup the user accounts for the Encoder/Decoder, click **User Accounts** in the Administration folder. The **User Configuration** window will be displayed as shown.



NOTE

Below is the default user account shipped from the factory:
User Name: Administrator
Password: Administrator
PIN: 2345

Select User - Select a user account from the dropdown list.

Add button - Create a new user account.

Delete button - Delete the selected user account. A confirmation page will be displayed. Click **Yes** to delete the user account or **No** to exit without deleting the user.

User Settings

Selected User

User Name: Administrator | PIN: •••• | Confirm PIN: ••••

Password: •••••••••••••••••••• | Confirm Password: ••••••••••••••••••••

Description: Administrator2

Username – Enter the username for the Account. The username must be unique and cannot be changed after the account is created. To change the username of an existing account, delete the account and create a new account.

> **NOTE**
> ***The username can only include alphanumerics. It cannot include any spaces or special characters.***

Password – Enter the password for the user account. The password must be between 4 and 32 characters long, and must adhere to the password complexity rules setup in the account preferences.

Confirm Password – Enter the password again for verification.

> **NOTE**
> ***The password cannot include spaces or any of the following characters: &, %, ‘, “, /, or \.***

PIN – Enter the PIN (Personal Identification Number) for the User account into this field. The PIN must be between 4 and 8 digits (numeric digits only) and must be unique.

Confirm PIN – Enter the PIN again for verification.

Description – Enter a description for this user account.

Locations

Check the locations for the selected user account. These locations are used when the user generates EAS messages. At least one location must be configured if the selected user has permission to use the Telephone interface.

Locations

	FIPS	County	State
☑	018000	All of Indiana	Indiana
☐	018003	Allen	Indiana
☑	018011	Boone	Indiana
☐	018013	Brown	Indiana
☐	018023	Clinton	Indiana

Roles

Configuration – Allow the user to make changes to the EASyCAP® configuration. This role must be enabled for any user that needs access to the front panel menu.

Configure Users – Allow the user to make changes to all user accounts. Note that any user can change their own password and PIN at any time regardless of the user account role.

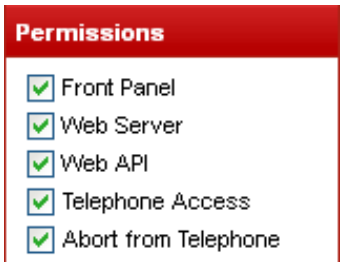
Upgrade Software – Allow the user to upgrade the EASyCAP® Encoder/Decoder software.

System Tests – Allow the user to perform calibration and system tests.

Generate EAS – Allow the user to generate EAS messages.

Generate Messages – Allow the user to generate custom (not EAS) messages.

Permissions



Front Panel – The user is allowed to access the front panel menu.

Web Server – The user is allowed access to the Web Server GUI interface.

Web API – The user is allowed access to the Web API interface. The **Web API** includes REST and CGI interfaces for monitoring status and performing specific operations.

Telephone Access – The user is allowed access to the touch-tone telephone interface.

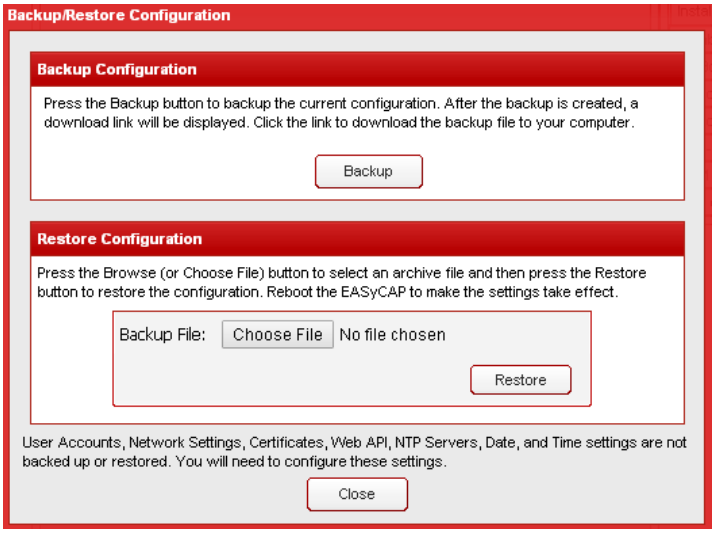
Abort from Telephone – The user is allowed to abort messages in progress from the touch-tone telephone interface.

Select the **Save** button to save changes to the User Account.

Select the **Close** button to close the User Configuration screen.

If changes were not saved before selecting **Close**, a dialog will be displayed. Select **No** to return to the User Configuration screen, or **Yes** to exit without saving changes.

Backup/Restore Configuration



To Backup or Restore the EASyCAP® configuration, select the **Backup/ Restore Configuration** link in the **Administration** folder.

Click the **Backup** button to backup the current EASyCAP® configuration. A new link will appear above the button. Click the ***Click here to download the backup file*** link. When the Save dialog appears, navigate to the desired directory on your PC and click **Save**.

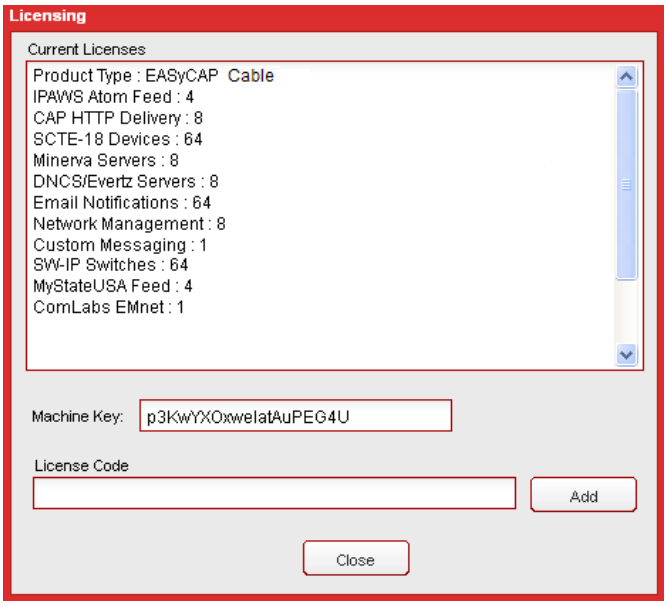
Click the **Browse** (or **Choose File**) button to restore a configuration backup. Select the desired configuration backup file and click **Open.** Then click the **Restore** button. A dialog will appear asking if you want to reboot. The restored configuration will not take effect until the EASyCAP® is rebooted.

Click **Close** to exit the **Backup/Restore Configuration** screen.

NOTE

User accounts, Network settings, Certificates, Web API, NTP servers, Date, and Time settings are not backed up or restored.

Licensing



To view and add Licenses, select **Licensing** in the **Administration** folder.

All installed licenses will be displayed.

To add a license, contact EAS Customer Support and provide them with the **Machine Key** shown on this screen. They will provide a **License Code**. Enter this code into the **License Code** field and click the **Add** button.

NOTE: Reboot the EASyCAP® after adding a new license in order for the licensed feature to become available.

Upgrade

To upgrade the EASyCAP® software, select the **Upgrade** link in the **Administration** folder.

NOTE

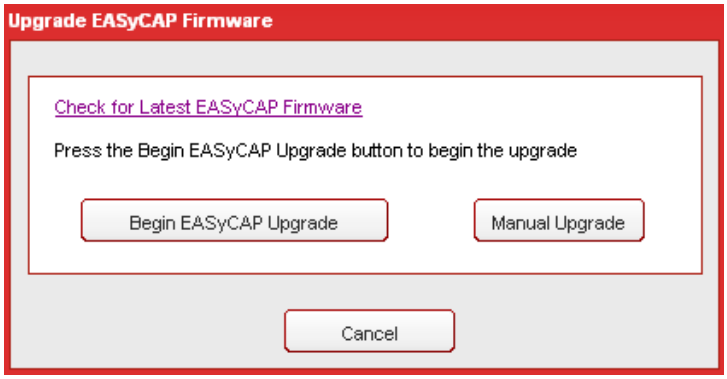
You should enable SSH on one of the Network Interfaces during software upgrades. SSH can be used to troubleshoot and correct problems in case errors occur during the upgrade.

NOTE

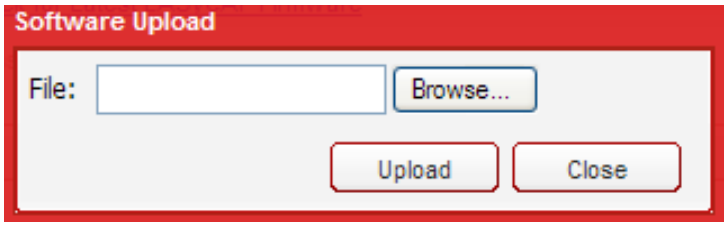
Most upgrades include updates for the EASyCAP® software and operating system updates. Upgrade EASyCAP® software first and then reboot and install the Linux updates.

Press the **Begin EASyCAP Upgrade** button to start the software upgrade. This will begin a step-by-step process to guide you through the upgrade.

The **Manual Upgrade** button should not be used. It is only provided to allow the upgrade file to be uploaded manually if errors occur during the upgrade.

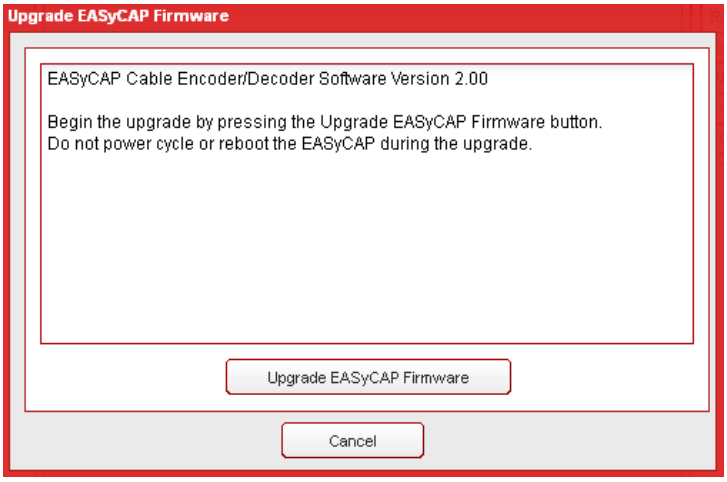


The **Software Upload** screen is shown after beginning the upgrade. Press the **Browse** (or **Choose File**) button. An **Open** (or **File Upload**) dialog box will appear. Choose the upgrade file and then press the **Open** button. Press the **Upload** button to upload the file to the EASyCAP®.



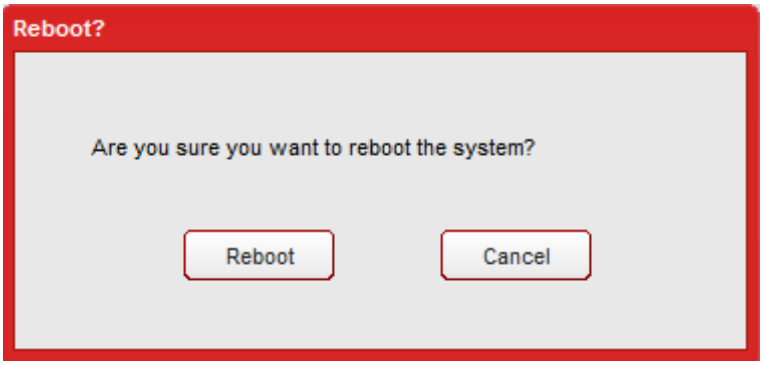
After the file is uploaded, package information and instructions will be shown. Press the **Upgrade EASyCAP Firmware** button to install the upgrade or select the **Close** button to exit without upgrading.

After the upgrade has completed, you will be prompted to reboot the EASyCAP®. Always reboot after installing an upgrade.



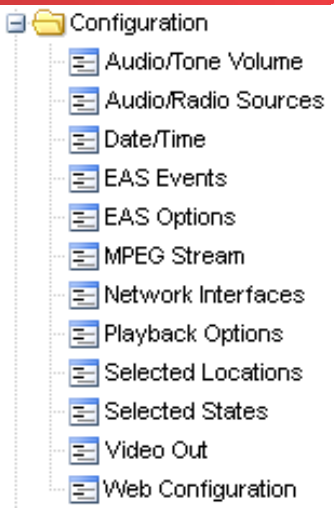
Reboot

To reboot the EASyCAP® Encoder/Decoder, select **Reboot** in the Administration folder. The **Reboot** dialog box will appear. Click **Reboot** to restart the EASyCAP® Encoder/Decoder. Click **Cancel** to exit without rebooting the EASyCAP® Encoder/Decoder.



Configuration Folder

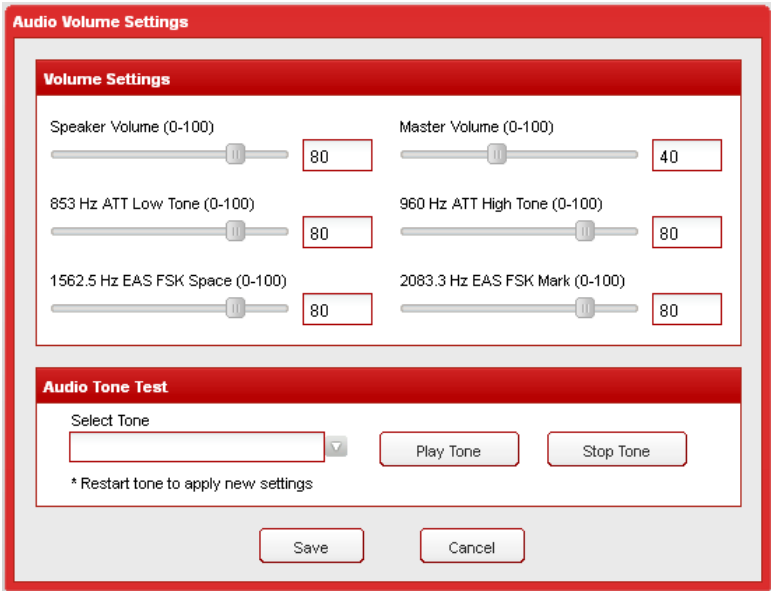
Expand the **Configuration** folder in the Navigation bar by clicking the **+** sign next to the **Configuration** folder.



Audio/Tone Volume

To setup the Audio/Tone Volume for the Encoder/Decoder, click **Audio/Tone Volume**. The **Audio Volume Settings** window will appear.

Volume Settings



Speaker Volume – Enter the output volume of the front panel speaker and line output (0-100). The default is 80.

Master Volume – Enter the maximum possible output volume (0-100) of all EASyCAP® audio outputs, with the exception of the front panel speaker. The desired volume of the alert voice audio should be used in determining the Master Volume setting (default is 40).

The Attention tone includes an 853Hz tone and a 960Hz tone. These tones are additive and need be set to the same output amplitude.

853 Hz ATT Low Tone – Sets the volume (0-100) for the 853 Hz tone that's used to generate the Attention tone (The default is 40). This setting should be set to half the desired Attention tone volume and should be the same volume as the 960 Hz tone.

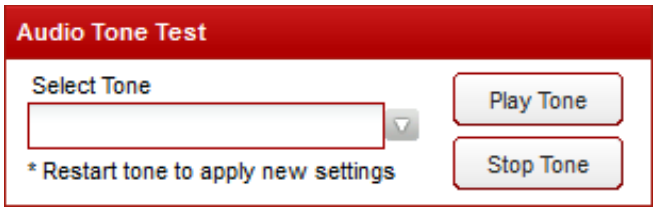
960 Hz ATT High Tone – Sets the volume (0-100) for the 960 Hz tone that's used to generate the Attention tone (The default is 40). This setting should be set to half the desired Attention tone volume and should be the same volume as the 853 Hz tone.

The generated EAS FSK uses 1562.5 Hz for its space frequency and 2083 Hz for its mark frequency. Theses tones are not additive, only one is used at a time. Set these two tones to the desired output amplitude, making sure they have the same amplitude.

1562.5 Hz EAS FSK Space – Sets the volume (0-100) for the EAS FSK Space frequency (The default is 40). Set this to the desired volume of the generated EAS FSK and make sure its output amplitude is the same as the 2083 Hz tone.

2083 Hz EAS FSK Mark – Sets the volume (0-100) for the EAS FSK Mark frequency (The default is 40). Set this to the desired volume of the generated EAS FSK and make sure its output amplitude is the same as the 1562.5 Hz tone.

Audio Tone Test



The Audio Tone Test is provided to allow the operator to calibrate the generated tones and setup the EASyCAP® audio output levels to match the normal program audio volume. During the test, the selected tone will be generated at the configured volume. The audio will be present at all of the EASyCAP® audio outputs and the program audio switch will be activated.

Select Tone – Select the desired tone/output to test from the drop-down menu.

Master Volume – Used to setup and test the Master volume, a 1050 Hz tone will be generated at the configured Master volume.

Attention Tone – Used to setup and test the 853 Hz and 960 Hz tones. An Attention tone will be generated at the configured volumes for the 853 Hz and 960 Hz tones.

853 Hz (ATT Low Tone) – Used to setup and test the 853 Hz tone, an 853 Hz tone will be generate at the configured volume. This tone is combined with the 960 Hz tone to make the Attention Tone, and will therefore be at half the amplitude of the Attention Tone.

960 Hz (ATT High Tone) – Used to setup and test the 960 Hz tone, a 960 Hz tone will be generate at the configured volume. This tone is combined with the 853 Hz tone to make the Attention Tone, and will therefore be at half the amplitude of the Attention Tone.

1562.5 Hz (EAS FSK Space) – Used to setup and test the 1562.5 Hz tone (EAS FSK Space frequency). A 1562.5 Hz tone will be generate at the configured volume. The volume will be equivalent to the generated EAS FSK.

2083.3 Hz (FSK Mark) – Used to setup and test the 2083 Hz tone (EAS FSK Mark frequency). A 2083 Hz tone will be generate at the configured volume. The volume will be equivalent to the generated EAS FSK.

Play Tone – Click this button to begin the audio tone test.

Stop Tone – Click this button to stop the audio tone test. It will stop the tone and return the program audio switch to passing normal program audio.

Select the **Save** button to save configuration changes or **Cancel** to exit without saving.

CAUTION

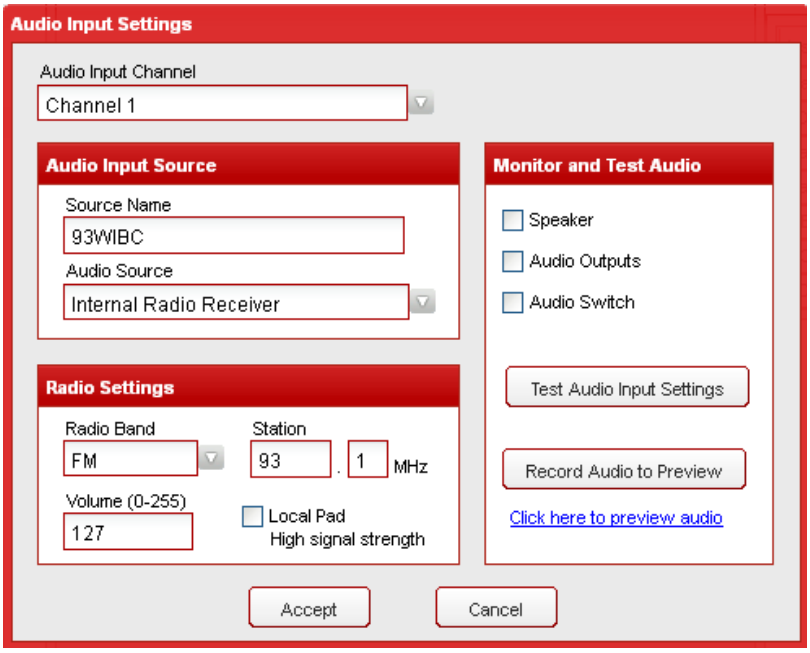
Your normal program may be interrupted during the audio test. The program audio switch will be activated and the test tone will be present at all of the EASyCAP® audio outputs.

NOTE

Any changes made to volume settings while a test is playing will not be reflected in the test. The test must be stopped, and the Play Tone button clicked again to reflect those changes.

Audio/Radios Sources

To configure the Audio Input Settings, click the **Audio/Radio Sources** link.



Audio Input Channel – Select which audio input to configure from the drop-down menu.

Audio Input Source

Audio Source – Select the audio input source from the dropdown menu as **Disabled**, an **External Audio Input** (baseband analog audio), or an **Internal Radio Receiver**.

Source Name – Enter a descriptive name to identify the audio input. This name will be displayed on the Front Panel LCD and in the Logs to identify the audio input channel.

Radio Settings

If the audio input is set to Internal Radio Receiver, the following Radio Settings apply:

Radio Band – Select the radio band (AM, FM, or NOAA) from the drop-down menu.

Station – Enter the frequency of the radio station

Volume – Enter the radio receiver volume. This should be left at the default value of 127 unless there is a problem with the audio level of the selected radio station.

Local Pad High signal strength – Check this box if the radio station is nearby and has a very strong signal strength. This should normally be left unchecked. When checked, the signal from the antenna will be padded down by 20dB.

NOTE

Setting the Radio volume to zero effectively disables that input.

Monitor and Test Audio

The operator can monitor the selected audio input and test the configured radio station by selecting the audio output(s) to use for monitoring the audio input.

Speaker – When checked, audio from the selected input will be routed to the front panel Speaker and the Line Output.

Audio Outputs – When checked, audio from the selected input will be routed to the Audio Outputs (the two balanced audio outputs available on the back panel of the EASyCAP®).

Audio Switch – When checked, the Program Audio switch will be activated, passing the audio from the selected input to the output terminals of the Audio Switch.

NOTE

Checking Audio Switch may interrupt your normal program audio.

Test Audio Input Settings – Press this button to test the audio input settings. If a radio station is configured, it will tune to the selected station and pass the audio to the selected monitor output.

Record Audio Preview – This button allows you to monitor audio inputs remotely. Press this button to record 30 seconds of audio from the selected input. After recording the audio, a link will appear below the button. Press the **Click here to preview audio** link to download or listen to the recorded audio.

Accept – Press this button to save changes to the audio input settings and close the window.

Cancel – Press this button to discard changes made to the configuration and close the window.

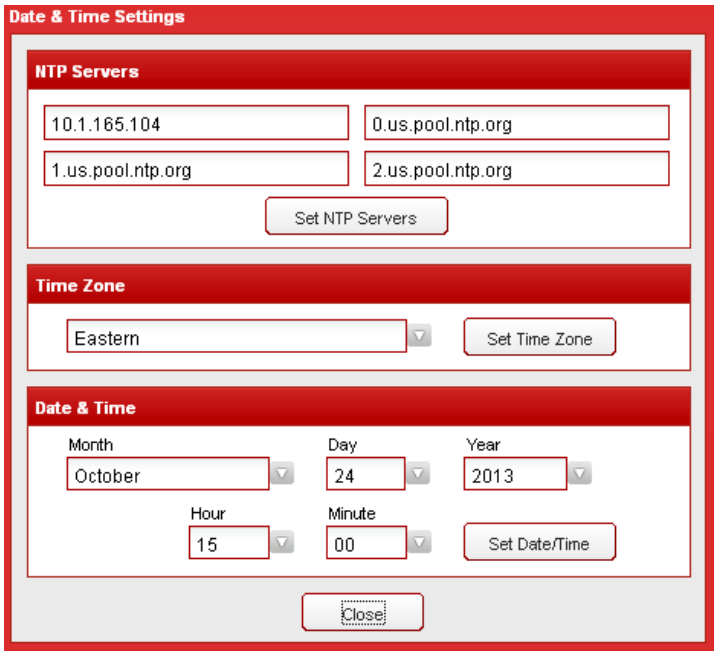
NOTE

Only Audio Inputs that are configured will be monitored for EAS alerts. By default, the EASyCAP® is configured to monitor all External Inputs.

Date/Time

To configure the Date/Time Settings for the EASyCAP® Encoder/Decoder, click the **Date/Time** link from the **Configuration** folder.

The following settings can be adjusted:



NTP Servers – Enter the URL or IP address of the Network Time Protocol servers. Click **Set NTP Servers** to save the changes.

Time Zone – Select the time zone from the dropdown list. Click **Set Time Zone** to save the changes to the time zone.

Month – Select the current month from the dropdown list.

Day – Select the current day from the dropdown list.

Year – Select the current year from the dropdown list.

Hour – Select the current hour from the dropdown list.

Minute – Select the current minute from the dropdown list.

Set Date/Time – Click the **Set Date/Time** button to apply the date and time settings.

Click **Close** when you have made all necessary adjustments.

NOTE

During initial configuration time and date should be set manually. Afterwards, if an NTP server is configured the date and time will automatically synchronize with the NTP server.

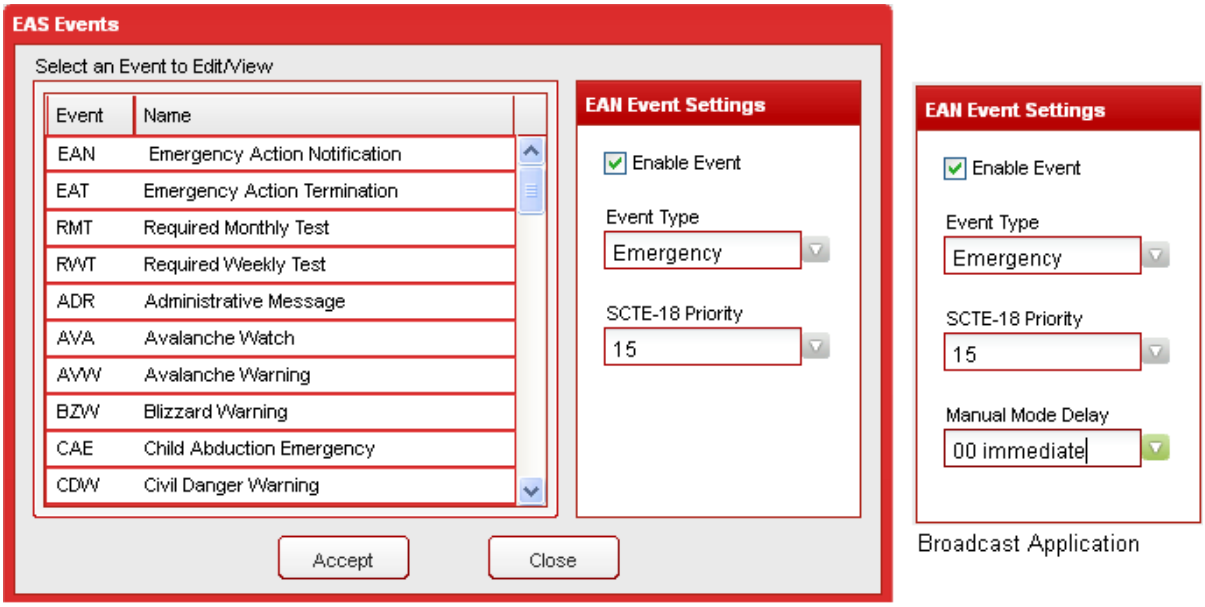
NOTE

If the time changes more than 15 minutes, the session will timeout and you will need to log back into the Web interface.

EAS Events

To configure EAS Events for the Encoder/Decoder, select the **EAS Events** link.

Click an event in the list to View and Edit its settings. The settings will be displayed in the **Event Settings** box on the right side of the window.

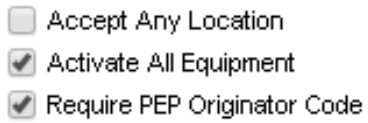


Cable TV Application

Broadcast Application

- **Enable Event** – Click this checkbox to enable the event. If the event is not enabled, the log will show when this type of event is received, but the alert will not be transmitted. The event can be manually generated regardless of whether it's enabled. EAN should always be enabled.
- **Event Type** – Select the type of event from the dropdown menu. The event type is used by some equipment to display different colors during message playback.
- **Priority** – Select the priority from the dropdown menu. This priority will be included in messages delivered to SCTE-18 recipients.
- **Manual Mode Delay (Broadcast Application only)** – Select the number of minutes to delay from the dropdown menu. When the Encoder/Decoder is in Manual mode, the alert playback will be delayed this amount of time, allowing the operator or automation equipment to confirm and begin the message playback. If the event is set to Indefinite, it will be allowed to expire while waiting for confirmation, otherwise the event will automatically begin playback if it is not confirmed or cancelled within the delay time. Note that the alert playback will automatically begin before the event expires regardless of the configured delay, unless it is set to Indefinite.

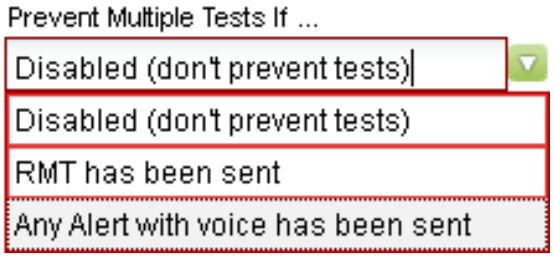
Three additional options are shown if the EAN event is selected.



- **Accept Any Location** – When enabled, an EAN will be accepted regardless of the included locations.
- **Activate All Equipment** – All downstream equipment will be activated, regardless of the configured location routing.
- **Require PEP Originator Code** – When enabled, an EAN will only be accepted if the Originator code is “PEP” (the EAN must be originated by a Primary Entry Point System).

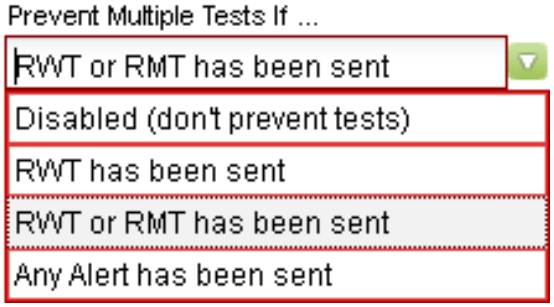
An option to **Prevent Multiple Tests** is available for Required Monthly Test and Required Weekly Test events (see testing rules in 47CFR11.61).

For a monthly test, the **Prevent Multiple Tests** option can be configured to prevent multiple RMT’s from being transmitted during the month, where a month is considered to be midnight of the first day of the month until 11:59:59 of the last day of the month.



- **Disabled** – Don’t prevent multiple monthly tests.
- **RMT has been sent** – Do not retransmit a received monthly test if an RMT was already transmitted during the month.
- **Any Alert with voice has been sent** – Do not retransmit a received monthly test if an alert that includes an attention tone and voice message was already transmitted during the month.

For a weekly test, the **Prevent Multiple Tests** option can be configured to prevent multiple RWT’s from being transmitted during the week, where a week is considered to be Sunday at midnight until Saturday at 11:59:59.



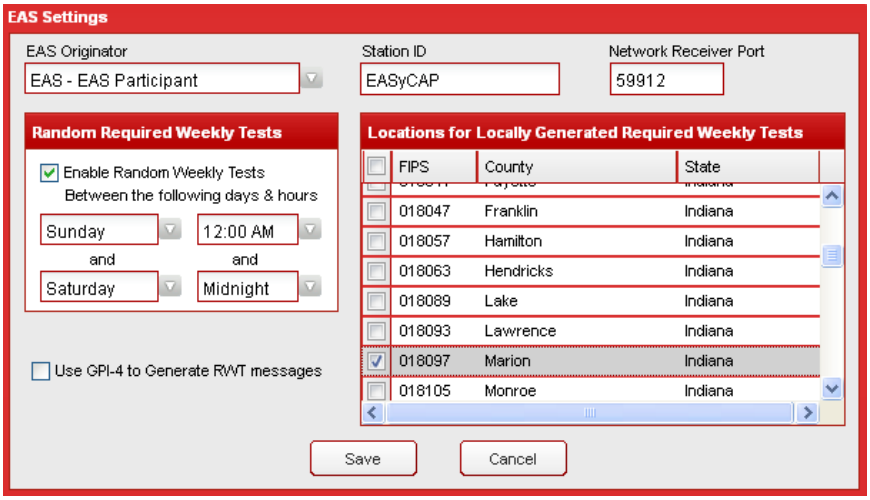
- **Disabled** – Don’t prevent multiple weekly tests.
- **RWT has been sent** – Do not retransmit a received weekly test if an RWT was already transmitted during the week.
- **RWT or RMT has been sent** – Do not retransmit a received weekly test if an RWT or an RMT was already transmitted during the week.
- **Any Alert has been sent** – Do not retransmit a received weekly test if an alert was already transmitted during the week.

Press the **Accept** button to save changes or the **Close** button to exit without saving.

EAS Options

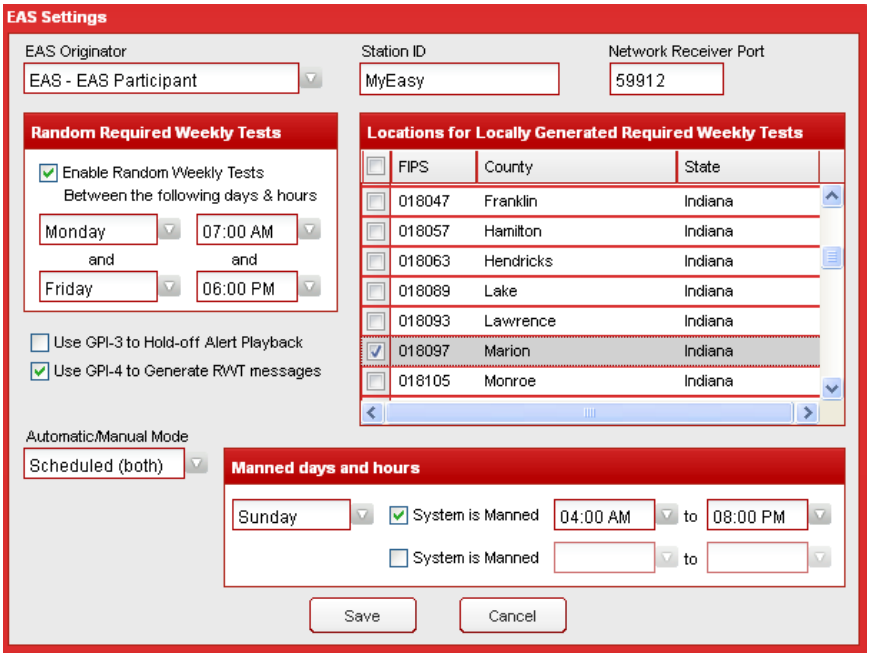
To configure EAS Settings of the Encoder/Decoder, select the **EAS Options** link in the **Configuration** folder. The **EAS Settings** window will be displayed.

EAS Settings



- **EAS Originator** – Select the appropriate originator code for your system, this is normally set to "EAS Participant."
- **Station ID** – Enter your station identification or call letters (up to 8 characters).
- **Network Receiver Port** – UDP port used to monitor for EAS messages from EASyIP Network Receiver's (default is 59912).
- **Random Required Weekly Tests** – These settings allow you to setup automatic generation of Required Weekly Tests. It is preferred that you manually generate RWT messages once a week, on a different day and at a different time, so that you can listen to it as it plays on your system. If this is not practical for your system, you can setup the EASyCAP® to automatically generate Required Weekly Tests.
    - Check the **Enable Random Weekly Tests** checkbox to enable the automatic generation of weekly tests.
    - Use the **Between the following days & hours** dropdown menus to configure the span of days and hours in which the Required Weekly Test can be generated.
- **Use GPI-4 to Generate RWT messages** – When this is checked, general purpose input 4 can be used to generate RWT messages.
- **Locations for Locally Generated Required Weekly Tests** – Select the locations that are included in locally generated RWT messages.

Settings for a Broadcast application



Use GPI-3 to Hold-off Alert Playback - checking this box will enable the use of general purpose input 3 to hold-off alert playback. It's intended to be used by automation equipment to delay the alert playback. If this input is not connected it needs to be disabled to prevent accidental delays with the alert playback.

Automatic/Manual Mode - Select the mode of operation from the dropdown menu.

Automatic Mode - Alerts are automatically forwarded when they're received. Select this option if you want to automatically forward alerts as they're received or if the system is not manned.

Manual Mode - When an alert is received, the EASyCAP® will wait for operator confirmation before beginning the alert playback. The amount of time to wait is configured per event on the EAS Events screen. This should only be selected if the station is manned or automation equipment is connected and configured to confirm the alert playback.

Scheduled - automatically switches between Automatic and Manual mode per the configured schedule.

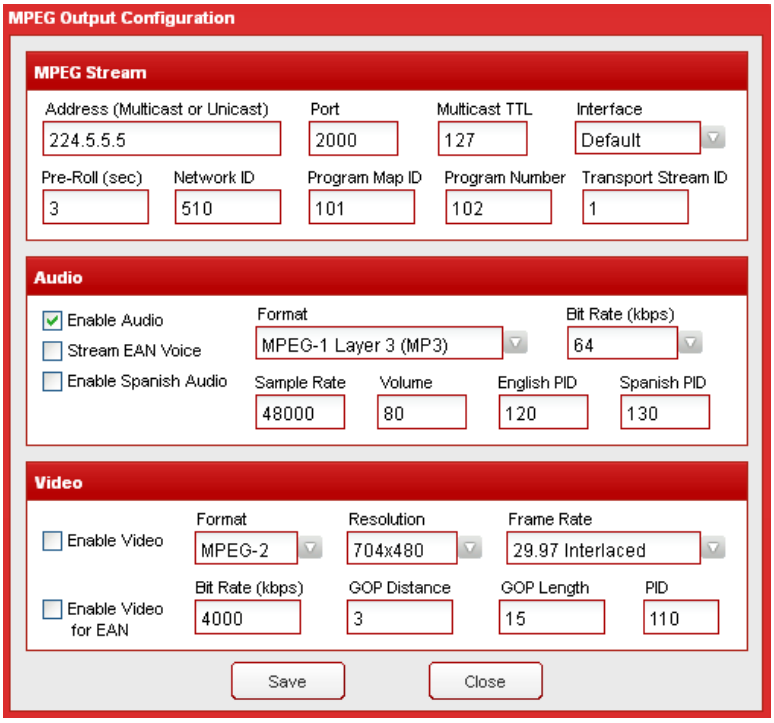
Manned days and hours - Provides the ability to setup a schedule for when the EASyCAP® runs in Manual mode. This is configured by selecting the day and the hours that the station is manned. Two shifts can be configured per day.

Select the **Save** button to save changes to the configuration or select the **Cancel** button to exit without saving any changes.

MPEG Stream

The EASyCAP® can stream MPEG-2 or MPEG-4 from any of the built-in Ethernet ports. The MPEG audio and video is encapsulated in an MPEG-2 transport stream and can be delivered to a unicast or multicast address. The MPEG stream can be used to create an "EAS Details" channel, eliminating the need for an external MPEG encoder. The MPEG stream is only present during the playback of EAS messages.

MPEG Stream



- **Address** – Enter the unicast or multicast address for the MPEG stream.
- **Port** – Enter the UDP port for the MPEG stream.
- **Multicast TTL** – Enter the time-to-live for the MPEG stream.
- **Interface** – Select the Ethernet interface to use for the MPEG stream. When set to "Default", network settings will determine which interface to use.
- **Pre-Roll** – The stream will start this many seconds before EASyCAP® begins playback. It is provided to help compensate for synchronization of the MPEG display due to processing or grooming delays.
- **Network ID** – Enter the original network ID of the transport stream.
- **Program Map ID** – Enter the program map PID.
- **Program Number** – Enter the program number.
- **Transport Stream ID** – Enter the transport stream ID.

Audio

- **Enable Audio** – Enable or disable audio for the MPEG stream.
- **Stream EAN Voice** – Enable/disable streaming the EAN voice message. If this option is disabled, only the FSK and attention tone audio will be streamed for an EAN.
- **Enable Spanish Audio** – Enable/disable streaming Spanish audio in the event a Spanish voice message is included with the EAS/CAP message.

- **Format** – Select the audio stream format as either MPEG-1 Layer 2 or Layer 3 (MP3).
- **Bit Rate** – Select the audio stream bitrate.
- **Sample Rate** – Enter the sample rate for the audio (8000-48000 Hz).

NOTE

If the bit rate is set to 16 kbps, the sample rate must be 8000 Hz

- **Volume** – Enter the volume for the audio (0 to 100). The default is 80.
- **English PID** – Enter the PID for the English audio.
- **Spanish PID** – Enter the PID for the Spanish audio.

Video

- **Enable Video** – Enable or disable MPEG video for the MPEG stream.
- **Enable Video for EAN** – Enable/disable video for an EAN. If video is disabled, this option provides the ability to stream video only for an EAN, which can be useful for systems that must force-tune to another channel during an EAN.
- **Format** – Select the video format as either MPEG-2 or MPEG-4 (H.264).
- **Resolution** – Select the video resolution (640x480, 704x480, or 720x480).
- **Frame Rate** – Select the video frame rate (29.97 or 30, interlaced or progressive).
- **PID** – Enter the PID for the video.

MPEG-2 video and compression options:

- **Bit Rate** – Enter the video bitrate in kbps.
- **GOP Distance** – Enter the distance between reference frames (I or P). For example, a distance of 3 would result in 2 B frames between reference frames. The default is 3.
- **GOP Length** – Enter the distance between I frames (1-30, 15 is the default).

MPEG-4 video and compression options:

- **Max Bit Rate** – Enter the maximum bitrate for the video in kbps.
- **Min Key Frames** – Enter the minimum distance between I frames (1-240, default is 15).
- **Max Key Frames** – Enter the maximum distance between I frames (1-240, default 30).

Press the **Accept** button to save changes or the **Close** button to exit without saving.

Network Configuration

CAUTION

Regardless of the network settings of the EASyCAP® Encoder/Decoder, a properly fire walled connection to the Internet is critical for the safe operation of this equipment. In addition, use of a reputable Internet provider and DNS Service may minimize risks associated with Internet access.

CAUTION

Hand editing the interfaces file may result in failure of the SSH and the Web interfaces. Use the Web Interfaces or front panel menu to change your network settings.

NOTE

Ethernet 1 and 2 are 1000 BASE-T ports.
Ethernet 3 and 4 are 100 BASE-T ports (on an optional board).
Use ports 1 and 2 for multicast and high bandwidth traffic.

NOTE

Ethernet ports 1-4 are equivalent to Linux devices eth0 - eth3. If an interface is referenced in an IProute command or script, make sure to use eth0 for Ethernet 1, eth1 for Ethernet 2, etc.

The EASyCAP® ships from the factory with the following network settings.

- Ethernet 1 is set to IP address 10.1.65.103 with a Subnet mask of 255.255.0.0.
- Ethernet 2 is set to IP address 192.168.1.102 with a Subnet mask of 255.255.255.0.
- Ethernet 3 is set to IP address 192.168.2.102 with a Subnet mask of 255.255.255.0.
- Ethernet 4 is set to IP address 192.168.3.102 with a Subnet mask of 255.255.255.0.
- HTTP, HTTPS, and SSH is enabled on both ports.

To setup the network settings for the EASyCAP®, select the **Network Interfaces** link.

The EASyCAP® Encoder/Decoder must be configured for network connectivity that allows Internet access to retrieve CAP messages and access to downstream equipment that is required to deliver alerts to subscribers. Additionally, management of the EASyCAP® Encoder/Decoder is provided by a Web Server, so inbound connections on port 443 and/or port 80 will be necessary.

Single Network Connection – The EASyCAP® Encoder/Decoder may be configured with only one Ethernet port enabled, relying on the system network for all connections to the Internet, required equipment, and web client (for management). In this configuration, the internal network is responsible for any necessary routing and security. In a very simple network of this kind, a router/gateway would allow outbound connectivity to the Internet while other equipment and a web client (PC) would be on the same IP subnet as the EASyCAP® Encoder/Decoder and therefore directly accessible.

Dual Network Connection – The EASyCAP® Encoder/Decoder may be configured with two Ethernet interfaces enabled allowing (typically) one interface to be used to access the Internet, while the other interface is used to access equipment and a web client (for management). In this configuration one interface may be configured with a default gateway pointing to an Internet router, while the other interface is either on the same subnet with the required equipment, or is configured with a (narrow) gateway to the equipment.

Two additional Ethernet interfaces can be added by installing an optional communications expansion board. These ports can be used to allow the Encoder/Decoder access to additional networks. These ports are 10/100 BaseT and should be used for connections that do not require high speeds.

Network Tab

Host Name – Enter the host name of the EASyCAP® Encoder/Decoder in this field.

DNS Server 1 – Enter the primary DNS server address in this field.

DNS Server 2 – Enter the secondary DNS server address in this field.

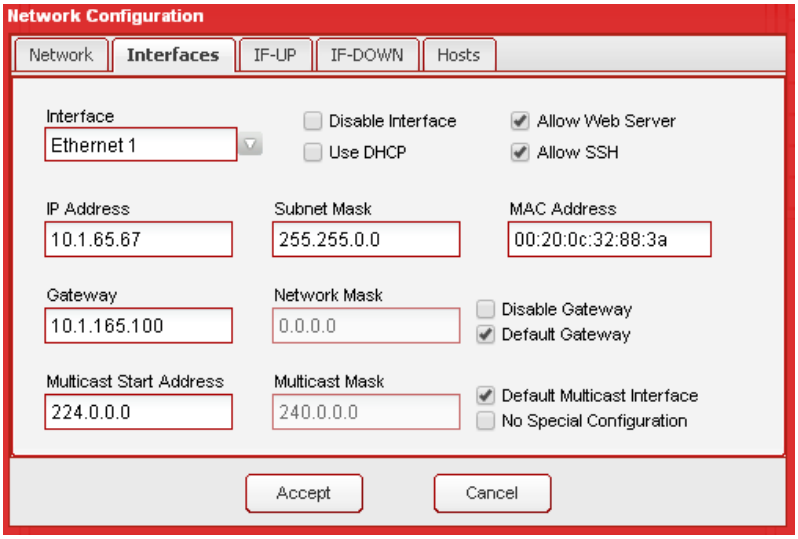
Generate SSH Certificate - Generate a new certificate for the SSH interface.

Interfaces Tab

Interface – Select the network interface to view or edit from this drop-down menu.

Disable Interface – Select this checkbox to disable the selected network interface.

Use DHCP – Select this checkbox to allow DHCP to automatically assign the address, subnet mask, and gateway to the selected network interface.



CAUTION

Use of DHCP on any interface may result in IP and gateway conflicts with the other interface, DNS conflicts, and other conflicts and ambiguities resulting in unreliable communication on both interfaces. Also, use of DHCP will enable the configuration HTTPS interface on all interfaces, regardless of the Allow Web Server settings for the interfaces.

Allow Web Server – Select this option to allow access to the Web Server from the selected network interface.

Allow SSH – Select this option to allow SSH access from the selected network interface.

IP Address – Enter the IP address for the selected interface.

Subnet Mask – Enter the subnet mask for the selected interface. Together with the IP address, this determines the subnet of the interface.

MAC Address – The MAC address of the selected network interface.

Disable Gateway – Disables the Gateway and Network Mask settings.

Default Gateway – Sets the Gateway to the widest possible network mask, making it the default when no narrower network exists on any interface.

CAUTION

Enabling a default gateway on more than one interface will result in unreliable communications.

Gateway – Enter the address of the router used to communicate with IP addresses that are not on the selected interfaces subnet, but are within the interfaces network. The **Gateway** IP address must be on the selected interfaces subnet.

Network Mask – Applying the **Network Mask** to the **Gateway** address will determine which addresses are routed through the **Gateway**. This determine the address range of the network in a manner similar to the way a Subnet Mask and IP Address determines what addresses are on the subnet.

Multicast Start Address and **Multicast Mask** – Enter the start address and mask for the multicast addresses that should be routed through the selected interface.

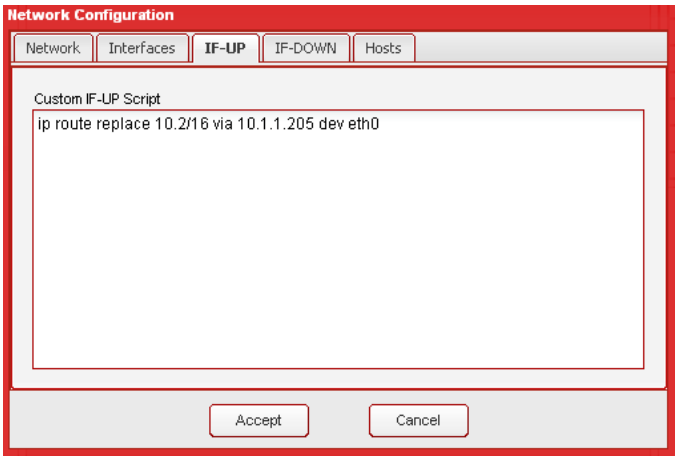
Default Multicast Address – Select this option to use the selected interface for multicast traffic that is outside of the multicast address range configured on other interfaces.

No Special Configuration – Select this option to disable any special configuration for multicast addresses on the selected interface.

IF-UP Tab

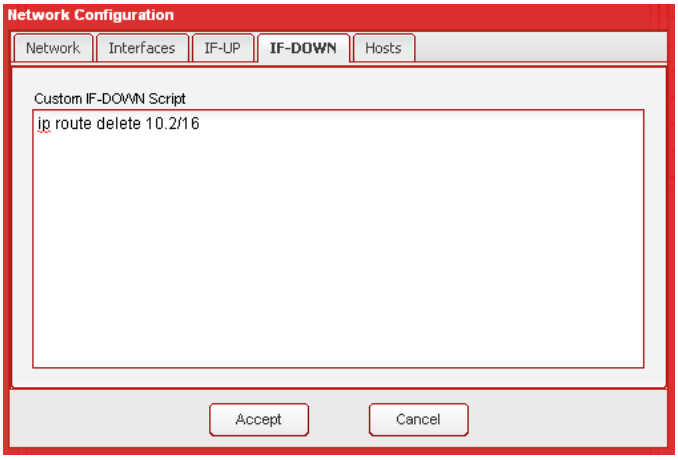
Custom IF-UP Script – This script provides a means for experienced users to hand-edit routes when a given interface is brought online. The $IFACE variable identifies the interface (eth0 or eth1). For example:

if ["$IFACE" = eth0]; then
ip addr add 10.2.10.5/24 brd + dev eth0
if



IF-DOWN Tab

Custom IF-DOWN Script – This script allows re-routing or removal of routes when an interface is going offline. The $IFACE variable identifies the interface going offline.

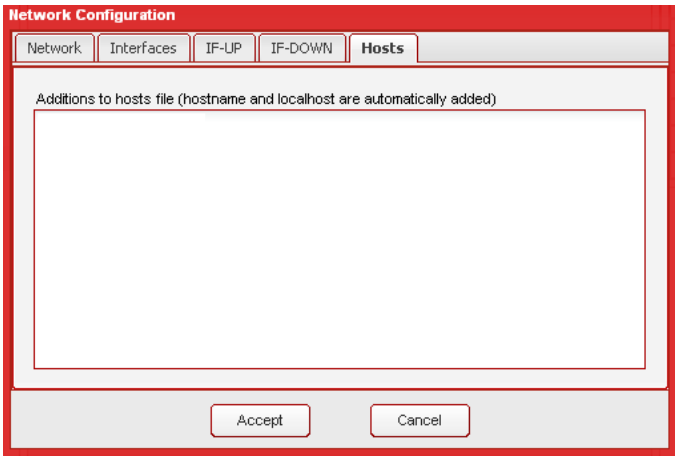


NOTE

The IProute2 Utility Suite (IP command) is recommended for IF-UP and IF-Down scripts.

Hosts Tab

Additions to hosts file – Enter any additional lines required in the hosts file. Do not enter lines for the hostname and localhost, this information will be added automatically.



Select the **Accept** button to save the network configuration.

Select the **Close** button to exit without saving changes to the configuration.

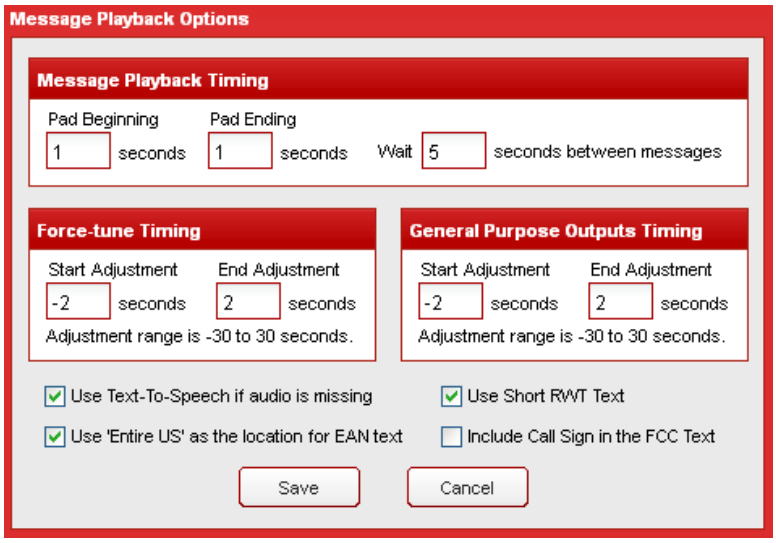
NOTE

If the EASyCAP IP address changed, you will need to close and then reopen your browser to login to the EASyCAP at the new IP Address.

Playback Options

To setup audio, text, and timing options, select the **Playback Options** link from the **Configuration** folder.

Message Playback Settings



- **Pad Beginning** – Enter the number of seconds to pad the start of playback. This adds silence to the beginning of audio and a static display to the video.
- **Pad Ending** – Enter the number of seconds to pad the end of playback, appending silence to the audio and a static display to the video.
- **Wait *n* seconds between messages** – Enter the number of seconds to wait between ending one message and starting the next message.

Force-tune Timing

These timing adjustments are provided for synchronization with systems that require time to encode MPEG streams and/or deliver downstream force-tune messages. For example, systems that use SCTE-18 messages to cause Set-tops to force-tune to an alternate channel.

- **Start Adjustment** – Enter the number of seconds to adjust delivery of messages to downstream equipment. A negative value causes force-tune messages to be sent before the EASyCAP® begins playback (static analog video is displayed and analog audio is silent before messages are sent). A positive value causes them to be sent after playback begins.
- **End Adjustment** – Enter the number of seconds to adjust the ending of messages delivered to downstream equipment. A negative value causes downstream messages to end before the EASyCAP® ends playback, and a positive value causes messages to end after playback has ended.

General Purpose Outputs Timing

These timing adjustments are not applicable to Broadcast applications. They only apply to the **Time Adjusted** general purpose outputs (onboard GPO-4 and all outputs from SW-IP switches). The adjustments are provided for synchronization with systems that require time to encode MPEG streams and/or deliver downstream messages, such as with an OM-1000.

- **Start Adjustment** – Enter the number of seconds to adjust activation of **Time Adjusted** and SW-IP outputs. A negative value activates outputs before the EASyCAP® begins playback (static analog video is displayed and analog audio is silent before activation). A positive value activates outputs after playback begins.
- **End Adjustment** – Enter the number of seconds to adjust the deactivation of **Time Adjusted** and SW-IP outputs. A negative value deactivates outputs before the EASyCAP® ends playback, and a positive value deactivates outputs after playback has ended.

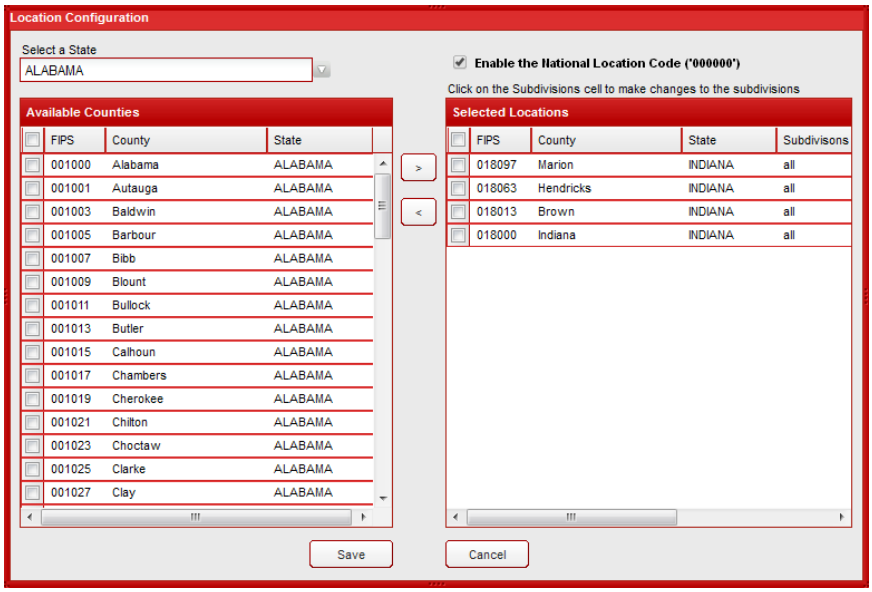
Audio/Text Options

- **Use Text-to-Speech if audio is missing** – When this box is selected, the EASyCAP® will generate speech from the text included in the alert message. Text-to-speech will only be generated if the message does not include English audio. This option only supports English audio.
- **Use Entire US as the location for EAN text** – When selected, the text for an EAN will show “Entire US” as the affected area.
- **Use Short RWT Text** – When selected, a short message will be used for Required Weekly Tests. For example: “A Required Weekly Test has been issued by an EAS Participant”.
- **Include Station ID** – When selected, your station identification (or Call Sign) will be included at the end of the alert text.

Select the **Save** button to save configuration changes or **Cancel** to exit without saving.

Selected Locations

To configure the locations serviced by your system, select the **Selected Locations** link in the **Configuration** folder. The **Location Configuration** page will be displayed.



The **Location Configuration** setup page is used to configure which EAS messages are processed, based on the areas affected by the alert. The selected Locations are used to determine which EAS alerts need to be processed. If no locations are selected, no alerts will be processed.

Adding Locations

First select a State from the Select a State dropdown box at the top of the window. Then, from the **Available Counties** display area, select the checkbox(es) that corresponds to the area(s) that you wish to add. Add the counties to the **Selected Locations** list by selecting the right arrow button.

Removing Locations

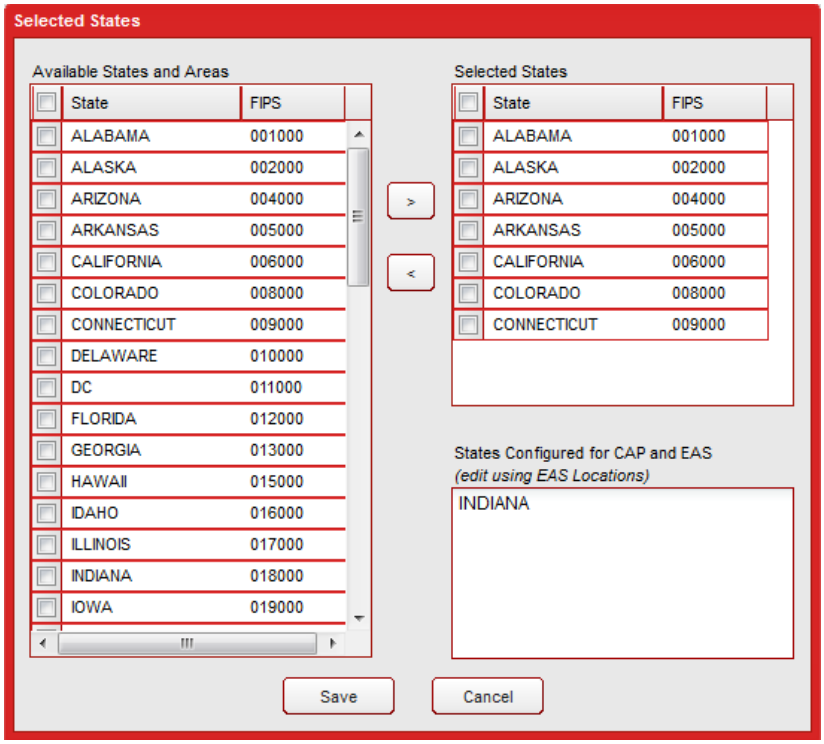
From the **Selected Locations** area, select the checkbox(es) that correspond to the location(s) that you wish to remove. Remove the location(s) from the **Selected Locations** display area by selecting the left arrow button.

Enable the National Location Code (000000) - When enabled, the six-zero National Location code will be accepted for all incoming messages.

Select the **Save** button to save the changes to the configuration or select the **Cancel** button to exit without saving the changes.

Selected States

To choose the states serviced by your system, select the **Selected States** link. The **Selected States** setup page will be displayed.



The **Selected States** setup page is used to configure which messages are processed, based on the areas affected by the alert. The IPAWS Atom Feed includes alerts for the entire United States, the selected States are used to determine which alerts need to be processed. Warning: If no states are selected, no alerts will be processed.

Adding States

From the **Available States and Areas** display area, select the checkbox(es) that corresponds to the state(s) that you wish to add. Add the states to the **Selected States** display area by selecting the right arrow button.

Removing States

From the **Selected States** area, select the checkbox(es) that correspond to the state(s) that you wish to remove. Remove the states from the **Selected States** display area by selecting the left arrow button.

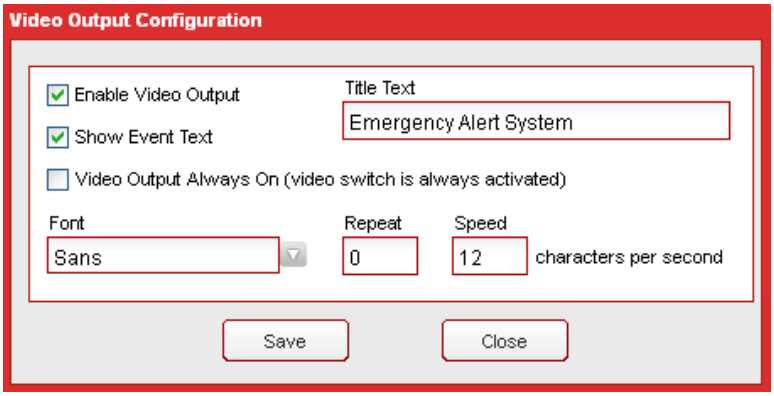
Press the **Save button** to save configuration changes, or click **Cancel** to exit without saving changes.

NOTE

The list of States Configured for CAP and EAS show required states. These states are automatically added when configuring the Selected Locations and cannot be deleted until every county within the state is deleted from the Selected Locations.

Video Out

To configure the analog video output of the Encoder/Decoder, select the **Video Out** link in the **Configuration** folder.

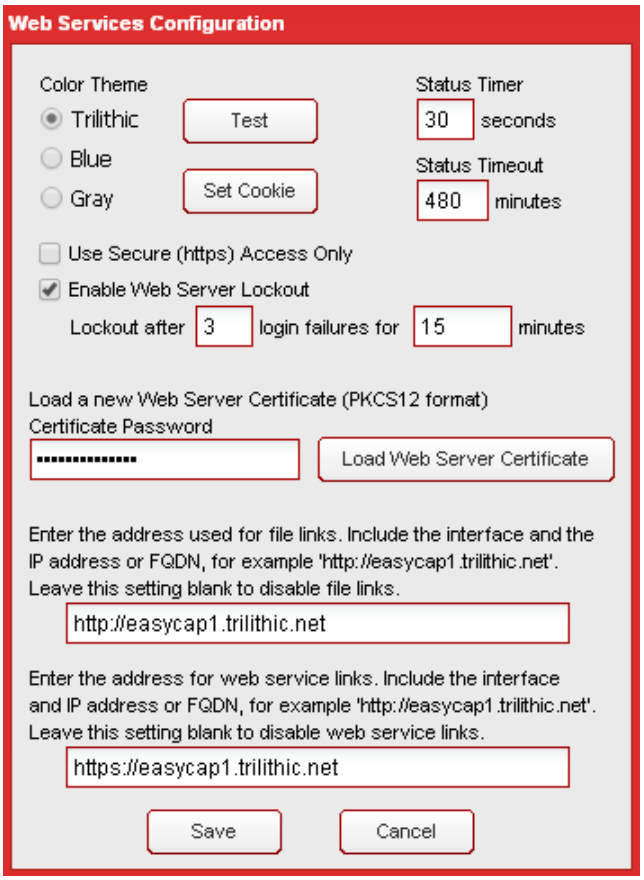


- **Enable Video Output** – Enable or disable the analog video output.
- **Show Event Text** – Select this option to display the name of the event (the type of alert, for example “Tornado Warning”).
- **Video Output Always On** – Select this option to provide a constant video source to downstream equipment. This will activate the video switch on startup and leave it active.
- **Title Text** – Enter text to use as a title for the video output. If text is entered, the top line of text displayed will be the configured title.
- **Font** – Select the font to use for the displayed text.
- **Repeat** – Enter the number of times to repeat the alert text on the video output (0-9). The text will always be repeated as many times as necessary to make it last at least as long as the audio (regardless of the configured repeat value).
- **Speed** – Enter the speed of the video message in characters per second (default is 12).

Click **Save** to save configuration changes, or click **Close** to exit without saving changes.

Web Configuration

To configure the EASyCAP® Encoder/ Decoder Web Services, select **Web Configuration** in the **Configuration** folder.



Color Theme – Click the radio button on the color theme you want to use. Click **Test** to view the color theme. Click **Set Cookie** to save the theme in a cookie for your local browser, which will override the global theme configured for the Web Server, allowing each user to have their own preference. Clicking Save will save the selected theme as the global theme for the Web Server.

Status Timer – Enter the number of seconds for the Status Monitor screen to poll for status updates.

Status Timeout – Enter the number of minutes that the Status Monitor screen can be active. After this timeout period the session will end, forcing a user logoff.

Use Secure (https) Access only – When enabled, only Secure (HTTPS) access to the EASyCAP® is allowed.

Web Server Lockout – If enabled, the Web server interface will be locked out for a configured amount of time after a configurable number of failed login attempts.

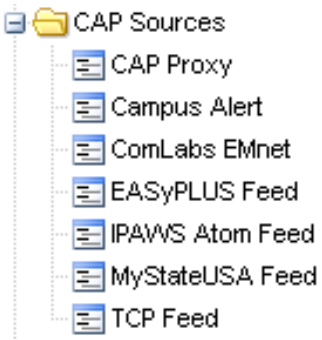
Web Server Certificate – The EASyCAP® ships with a self-signed certificate for the Web Server. To configure a different certificate, press the **Load Web Server Certificate** button and select the desired certificate. The certificate must use PKCS12 format. If the certificate is password protected, enter the password in the **Certificate Password** field. The Web Server will not be configured to use the new certificate until the **Save** button is pressed. Note that the **Use Secure Access Only** option will be disabled when a new certificate is configured to allow HTTP access until the certificate can be tested.

The **address used for File Links** and **Web Service Links** configures the address used for links that are included in outgoing Emails and SNMP. These addresses must begin with “https://” (or “http://”), for example “https://easycap1.trilithic.net”. If you do not want File or Web Service links to be included in Emails or SNMP, leave the setting blank.

Click **Save** to save configuration changes or click **Cancel** to exit without saving changes.

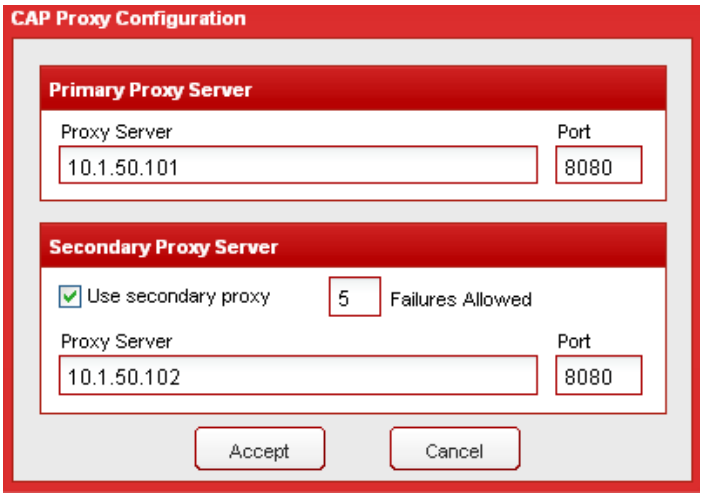
CAP Sources

Expand the **CAP Sources** folder in the Navigation bar by clicking the **+** sign next to the **CAP Sources** folder.



CAP Proxy Configuration

To configure CAP Proxy Servers, select the **CAP Proxy** link. The **CAP Proxy Configuration** setup page will be displayed.



Primary Proxy Server - This HTTP/HTTPS Proxy Server is used to retrieve CAP messages and audio files. Enter the Proxy Server as a fully qualified domain name or an IP address. Also enter the correct TCP port to use for the Proxy Server.

Use secondary proxy - Select this option to use a secondary proxy if the primary proxy fails. When enabled, if a configurable number of sequential failures occur while polling a CAP source, the software will failover (or fall back) to the alternate proxy. Note that any unexpected response from a CAP source will be considered a failure.

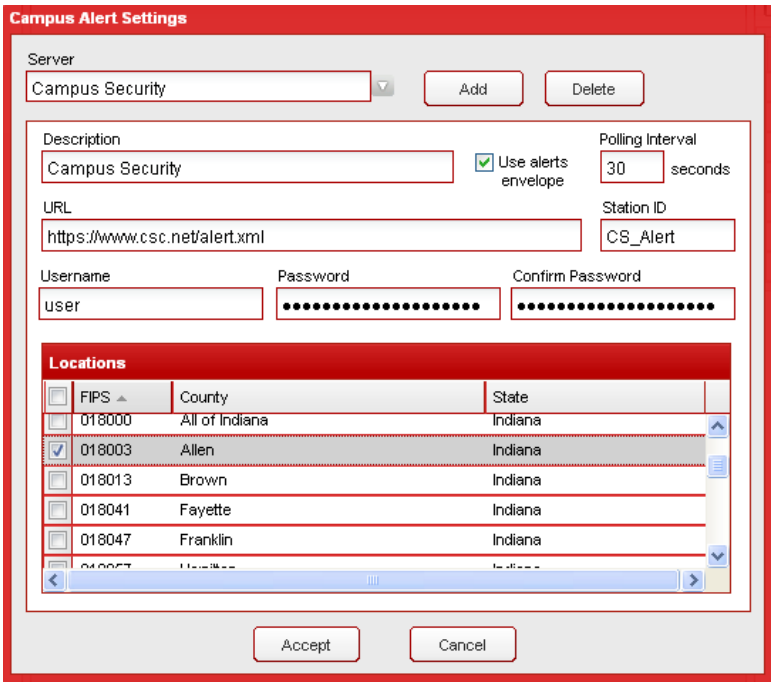
Failures Allowed - Enter the number of failures allowed before failing over to the alternate proxy (the default is 5).

Secondary Proxy Server - This HTTP/HTTPS Proxy Server is used as an alternate proxy when the CAP source cannot be polled through the primary proxy. It is only used when the **Use secondary proxy** option is enabled. Enter the proxy server as a fully qualified domain name or an IP address. Also enter the correct TCP port to use for the secondary proxy server.

Select the **Accept** button to save changes to the CAP Proxy configuration or select the **Cancel** button to exit without saving the changes.

Campus Alert Feed

The Campus Alert feed allows the EASyCAP® to retrieve CAP messages from Omnilert and Rave Mobile Safety servers. It can also be used for other CAP servers that provide a similar HTTP interface. These CAP messages are not IPAWS compliant, and are used to distribute alerts that effect a local area (like a college campus).



Server – Select a feed from the drop-down menu to view and edit.

- **Add** - Add a new feed.
- **Delete** - Delete the selected feed.

Feed Settings

- **Description** – Enter a description for this feed.
- **Use alerts envelope** – Select this checkbox if the feed uses an alerts envelope that can include more than one CAP message.
- **Polling Interval** – Enter the number of seconds between requests for new CAP messages.
- **URL** – Enter the URL. The CAP xml file should be included in the URL (for example "http://www.myuniversity.edu/alert.xml").
- **Station ID** – Enter a unique station ID for this feed (8 characters maximum). This is used to identify the source of received messages in the alert log.
- **Username** – Enter the username assigned by the CAP source administrator.
- **Password** – Enter the password assigned by the CAP source administrator.
- **Confirm Password** – Enter the password again for verification.
- **Locations** – Enter the areas effected by this feed. Campus Alert messages generally don't include locations, so user configuration provides the effected areas.

Press the **Accept** button to save configuration changes or select the **Cancel** button to exit without saving any changes.

ComLabs EMnet Client

The ComLabs EMnet Client allows the EASyCAP® to receive CAP messages from EMnet Internet and satellite sources. Systems that don't have Internet access can receive CAP messages via satellite. EMnet also provides increased reliability by offering a redundant path for CAP message delivery.

Select the **ComLabs EMnet** link from the **CAP Configuration** folder to configure and check the status of the EMnet client.

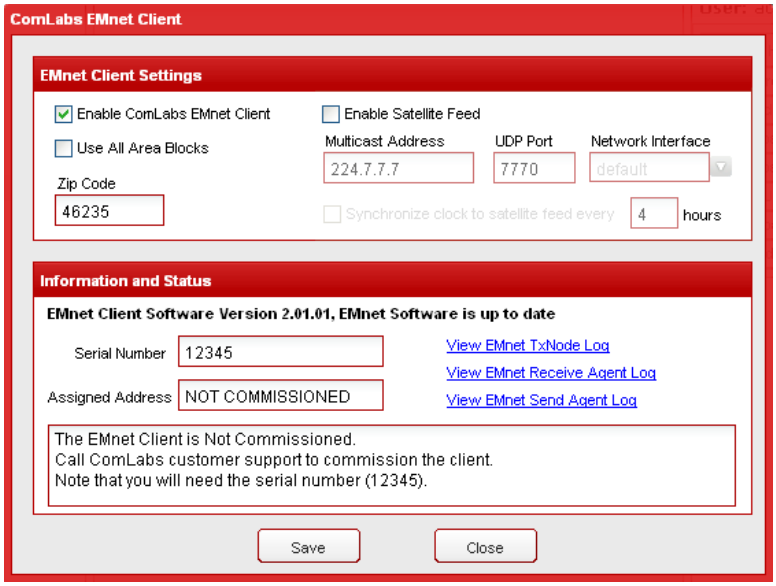
Licensing and Commissioning EMnet

EMnet must be licensed to run on the EASyCAP®. It must also be commissioned by ComLabs before it can receive CAP messages. This process is only required the first time the client software runs. Before running the EMnet client, make sure the following prerequisites are met.

- The EMnet client must be licensed (from the Administration/Licensing screen).
- The EASyCAP® must have access to the Internet or to a bidirectional satellite feed.
- The EASyCAP® must have a valid DNS configured.
- TCP ports 25, 22025, 110, and 22110 must be open (do not block these ports).

1) Enable the EMnet client by selecting the **Enable ComLabs EMnet Client** check-box.

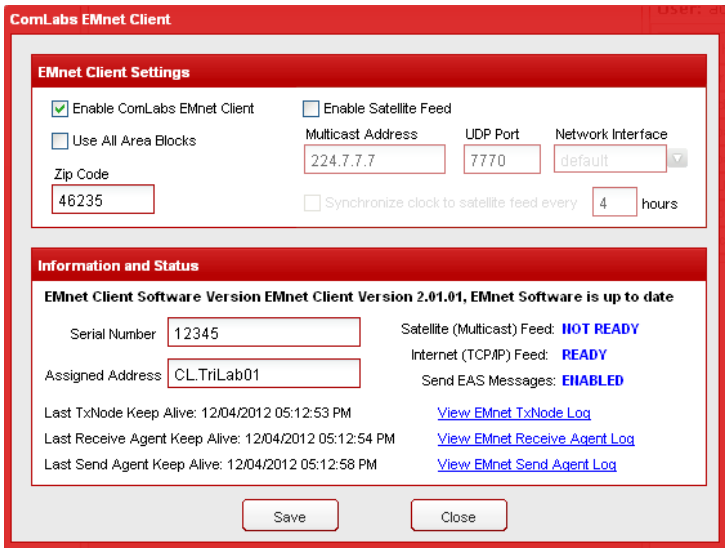
2) Press the **Save** button to save the configuration and start the EMnet client.



4) A valid serial number should be present in the **Serial Number** edit-box and a warning should be displayed about commissioning the software. If not, the most likely cause is that the client cannot contact a ComLabs server.

5) Contact ComLabs customer support to commission the client software. Note that you will need to give them the serial number (from the **Serial Number** edit-box).

EMnet Client Configuration



Enable ComLabs EMnet Client - Enable or disable the EMnet client with this check-box.

Use All Area Blocks - Select this check-box to process all <area> blocks within a CAP message. If disabled, only the first <area> block is used. Disabled this to comply with current CAP to EAS implementation guidelines.

Zip Code - Enter the Zip Code for your service area in this edit-box.

Enable Satellite Feed - Select this check-box to receive CAP messages from the EMnet satellite feed.

Multicast Address - Enter the multicast address of the satellite receiver.

UDP Port - Enter the UDP port used by the satellite receiver to deliver CAP messages.

Network Interface - Enter the physical network interface used to receive CAP messages from the satellite receiver. When this is set to **Default**, the software will try to use the default network interface (first interface enumerated into the system), and if that fails it will then try to acquire a connection using the other available network interface(s).

Synchronize clock to satellite every - Select this check-box to synchronize the EASyCAP system clock to the time reported by the satellite feed. Enter how often the clock should be synchronized in the **hours** edit-box. Disable this option if an NTP server is configured.

EMnet Client Information and Status

The status and system information of the EMnet client are displayed in this area. The **Serial Number** and **Assigned Address** uniquely identify this instance of the client. These are assigned and maintained by ComLabs. The **Serial Number** is required to commission the EMnet client.

The **Satellite (Multicast) Feed** and **Internet (TCP/IP) Feed** status indicate which sources are configured to receive EMnet CAP messages. At least one feed must have a status of ***READY*** in order to receive CAP messages from EMnet. The **EAS Messaging** status indicates if the EMnet client is configured to receive CAP messages. This should be ***ENABLED*** when ComLabs commissions the client.

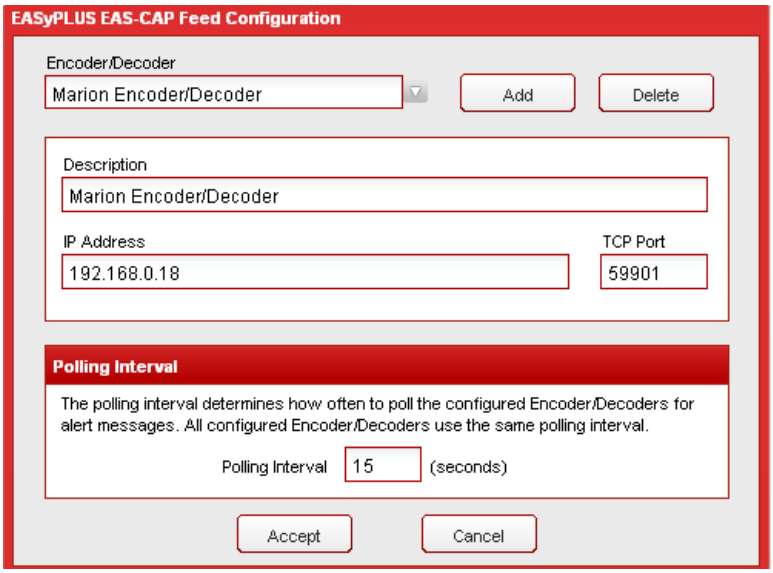
The keep alive times show the time of the last keep alive for each EMnet client process. Links are provided to view the log for each EMnet process. Click on the link to view the log.

Press the **Save** button to save configuration changes. Press the **Close** button to exit the EMnet client configuration page.

EASyPLUS EAS-CAP Feed

The EASyPLUS feed allows the EASyCAP® to retrieve EAS messages from EASyPLUS and EASyIP Encoder/Decoders.

To setup EASyPLUS EAS-CAP feeds, select the **EASyPLUS Feed** link from the **CAP Configuration** folder.



Encoder/Decoder – Select an EASyPLUS feed from the drop-down menu to view and edit its settings.

- **Add button** - Add a new EASyPLUS feed.
- **Delete button** - Delete the selected EASyPLUS feed. A confirmation dialog box will be displayed. Select the **Yes** button to delete the EASyPLUS feed or select the **No** button to exit without deleting the feed.

- **Polling Interval** – Enter the amount of time in seconds between each request for new alert messages from the EASyPLUS feeds. This is a global setting that applies to all of the configured EASyPLUS feeds.

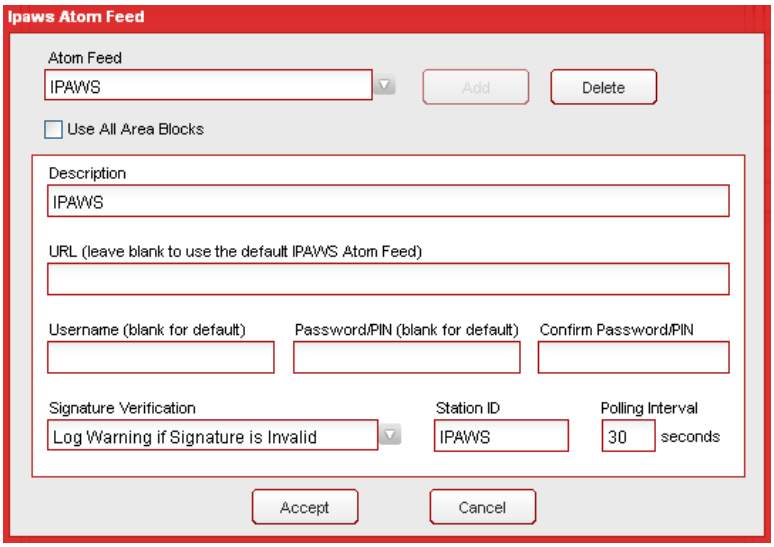
EASyPLUS EAS-CAP Feed Settings

- **Description** – Enter a description for this feed.
- **IP Address** – Enter the IP Address of the EASyPLUS into this field.
- **TCP Port** – Enter the TCP Port for the EASyPLUS feed, the default is 59901.

You can change the settings for multiple EASyPLUS EAS-CAP feeds before accepting (and saving) the changes. Once you're done configuring the EASyPLUS feeds, press the **Accept** button to save all of the changes made or select the **Cancel** button to exit without saving any changes.

IPAWS Atom Feed

The IPAWS Atom feed allows the EASyCAP® to retrieve CAP messages from the FEMA IPAWS Open Atom feed.



Atom Feed – Select a feed from the drop-down menu to view/edit.

- **Add** - Add a new Atom feed.
- **Delete** - Delete the selected Atom feed.

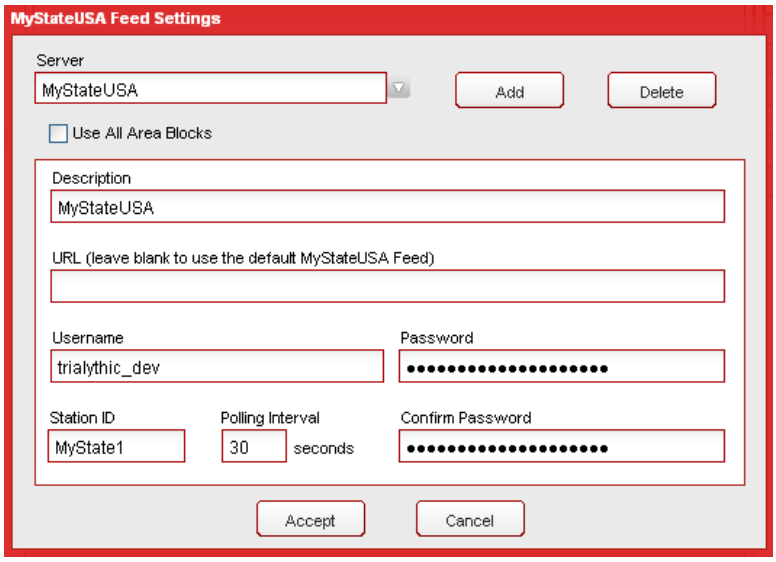
IPAWS Atom Feed Settings

- **Use All Area Blocks** – Select this option to process all <area> blocks in a CAP message. If disabled, only the first <area> block is processed. This should be disabled in order to comply with current CAP to EAS implementation guidelines.
- **Description** – Enter a description for this feed.
- **URL** – Enter the URL of the Atom feed into this field. Leave blank to use the default IPAWS Open Atom Feed URL.
- **Username** – If applicable, enter the username for the feed. FEMA's IPAWS Atom feed does not use a username, and this field should normally be left blank. If a username is configured, Basic authentication will be used.
- **Password or PIN** – Enter the password or PIN assigned by the CAP source administrator. Leave blank to use the default PIN for the IPAWS Atom feed.
- **Confirm Password/PIN** – Enter the password/PIN again for verification.
- **Signature Verification** – Select **Do Not Verify Signatures** to ignore the CAP messages digital signature. Select **Log Warning if Signature is Invalid** to log a warning if the digital signature is invalid. Select **Reject Message if Signature is Invalid** to reject messages when the digital signature is invalid.
- **Station ID** – Enter a unique station ID for this feed (8 characters maximum). This is used to identify the source of received messages in the alert log.
- **Polling Interval** – Enter the time in seconds between requests for new messages.

Press the **Accept** button to save changes, or select the **Cancel** to exit without saving.

MyStateUSA Feed

The MyStateUSA feed allows the EASyCAP® to retrieve CAP messages from MyStateUSA CAP servers. It can also be used for other CAP servers that provide a similar HTTP interface.



Server – Select a MyStateUSA feed from the drop-down menu to view and edit its settings.

- **Add button** - Add a new MyStateUSA feed.
- **Delete button** - Delete the selected MyStateUSA feed.

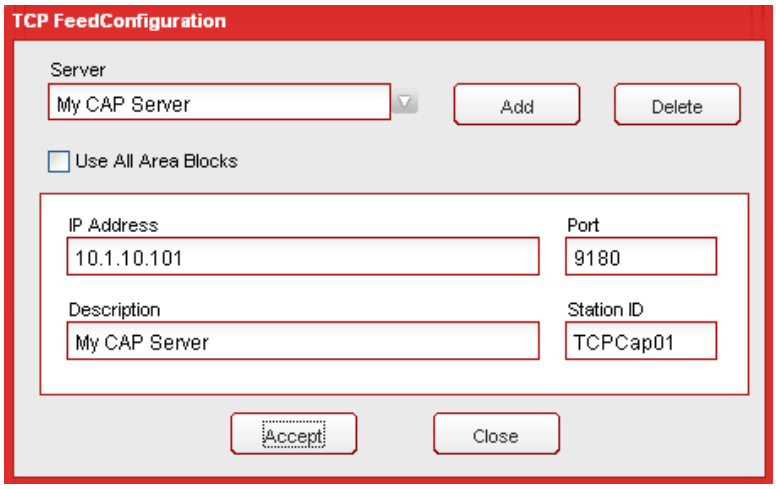
MyStateUSA Feed Settings

- **Use All Area Blocks** – Select this option to process all <area> blocks within a CAP message. If disabled, only the first <area> block will be processed. This should be disabled in order to comply with current CAP to EAS implementation guidelines.
- **Description** – Enter a description for this feed.
- **URL** – Enter the URL of the MyStateUSA Feed into this field. Leave this field blank to use the default MyStateUSA URL.
- **Username** – Enter the username assigned by the CAP source administrator.
- **Password** – Enter the password assigned by the CAP source administrator.
- **Confirm Password** – Enter the password again for verification.
- **Station ID** – Enter a unique station ID for this feed (8 characters maximum). This is used to identify the source of received messages in the alert log.
- **Polling Interval** – Enter the amount of time in seconds between each request for new CAP messages.

You can change the settings for multiple MyStateUSA feeds before accepting (and saving) the changes. Once finished configuring the IPAWS feeds, press the **Accept** button to save all of the changes made or select the **Cancel** button to exit without saving any changes.

TCP Feed

To setup TCP feeds, select the **TCP Feed** link from the **CAP Configuration** folder.



Server – Select a TCP feed from the drop-down menu to view and edit its settings.

- **Add button** - Add a new TCP feed.
- **Delete button** - Delete the selected TCP feed.

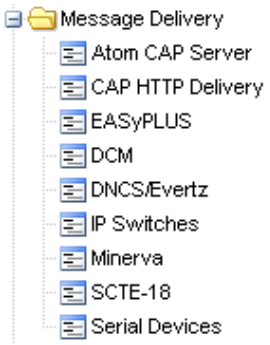
TCP Feed Settings

- **Use All Area Blocks** – Select this option to process all <area> blocks within a CAP message. If disabled, only the first <area> block will be processed. This should be disabled in order to comply with current CAP to EAS implementation guidelines.
- **IP Address** – Enter the IP Address of the TCP feed into this field.
- **Port** – Enter the TCP port number.
- **Description** – Enter a description for this feed.
- **Station ID** – Enter a unique station ID for this feed (8 characters maximum). This is used to identify the source of received messages in the alert log.

You can change the settings for multiple TCP Feeds before accepting (and saving) the changes. Once you're done configuring the TCP Feeds, press the **Accept** button to save all of the changes made or select the **Cancel** button to exit without saving any changes.

Message Delivery Folder

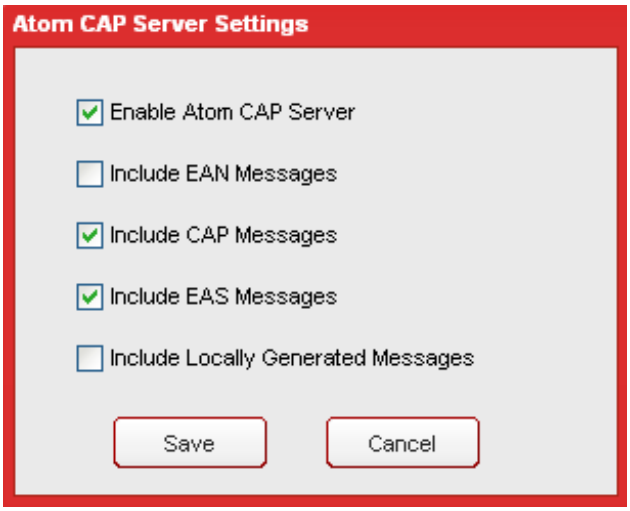
Expand the **Message Delivery** folder in the Navigation bar by clicking the **+** sign next to the folder.



Atom CAP Server

The Atom CAP Server feature provides a CAP feed similar to FEMA's IPAWS Open Atom feed, allowing downstream Encoder/Decoder's to retrieve IPAWS compliant CAP messages from the EASyCAP®. This feature provides the ability to transfer CAP and EAS messages to other EASyCAP® Encoder/Decoder's. Messages received via EAS are formatted into IPAWS compliant CAP messages and then made available on the Atom feed.

Select the **Atom CAP Server** link from the **Message Delivery** folder to setup the server.



Enable Atom CAP Server – Enable or disable the Atom CAP Server.

Include EAN Messages – Include EAN messages on the Atom feed.

- If the EAN is received from an EAS source, the audio stream URI will reference an audio stream hosted by the EASyCAP®.
- EAN messages received from CAP sources will not be available on this feed.

Include CAP Messages – Include message received via CAP sources on the Atom feed.

Include EAS Messages – Include message received via EAS sources on the Atom feed. This includes messages received via audio and radio sources, Network Receiver's, and EASyPLUS Encoder/Decoder's.

Include Locally Generated Messages – Include message that were locally generated (by an operator or the random weekly test generator) on the Atom feed.

Press **Accept** to save configuration changes or **Cancel** to exit without saving any changes.

Configure user accounts for the Atom CAP Server:
At least one user account needs to be configured to allow access to the **Atom CAP Server**. The user account must have the **Web API** permission enabled in order to login to the **Atom CAP Server**.

Configuring client's to receive messages from the Atom CAP Server:
The client side configuration is similar to configuring FEMA's IPAWS Open Atom feed.

1) Add an IPAWS Atom Feed.

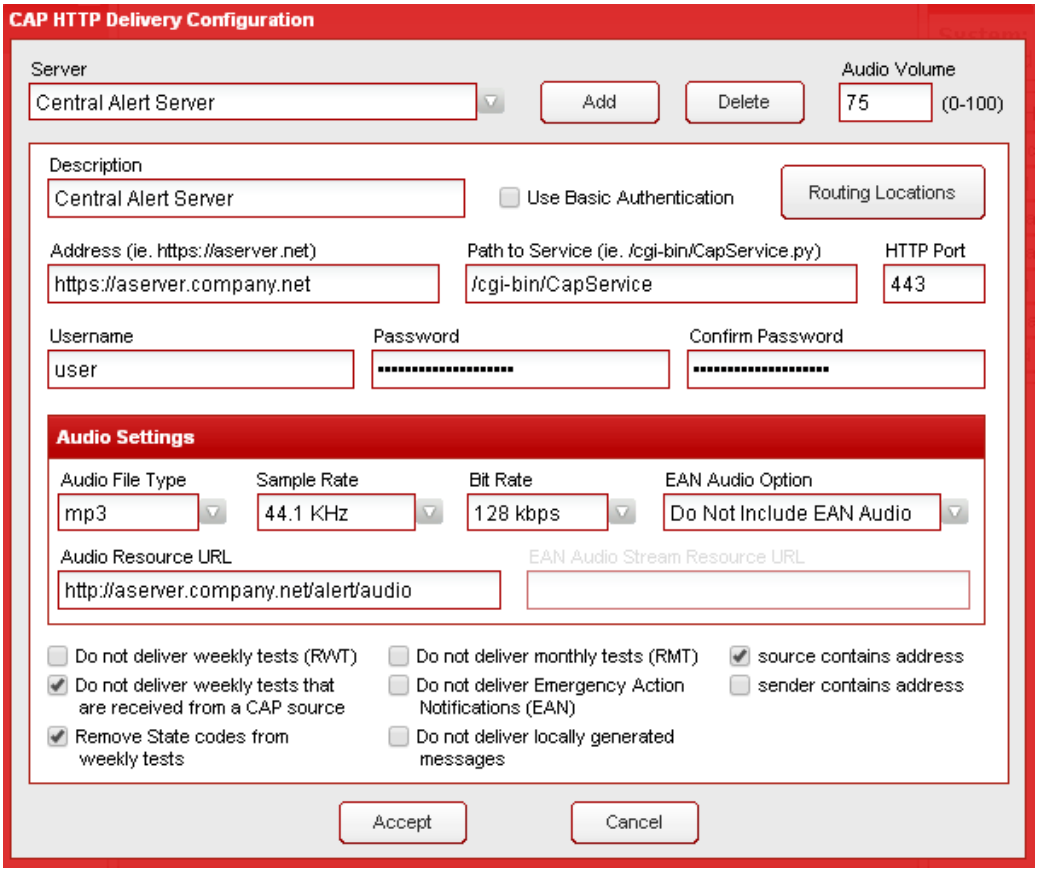
2) The URL is configured as the HTTPS address of the EASyCAP® followed by "EASCAP_EAS_SERVICE/rest". For example, if the EASyCAP address is 192.168.1.71, the URL is: https://192.168.1.71/EASCAP_EAS_SERVICE/rest.

3) Enter the username and password of the user account that was setup for the **Atom CAP Server.** The server uses Basic Authentication, therefore the username and password are required.

CAP HTTP Delivery

The CAP HTTP Delivery feature provides the ability to deliver EAS and CAP messages to HTTP/HTTPS servers. All alert messages are formatted into IPAWS compliant CAP messages prior to delivery. CAP messages and audio are delivered via a single HTTP Post, using multipart form data.

To setup the delivery of CAP messages to HTTP/HTTPS servers, select the **CAP HTTP Delivery** link from the **Message Delivery** folder.



Server – Select a server from the drop-down menu to view and edit its settings.

Add button - Add a new HTTP server.

Delete button - Delete the selected HTTP Server.

Audio Volume - Set the audio file volume (0-100).

Description – Enter a descriptive name for this server.

Use Basic Authentication – Select this option to use Basic Authentication. If Basic Authentication is not enabled, login information will be included in the multipart/form-data.

Address – Enter the protocol (http or https) and hostname or IP address of the server. For example: http://aserver.company.net.

Path to the Service – Enter the path to the web service. For example: /cgi-bin/capservice.

NOTE

The Address, HTTP Port, and Path to Service are combined to form the URL. If Address is http://aserver.company.net, HTTP Port is 80, and Path to Service is /cgi-bin/capservice, then the combined URL would be http://aserver.company.net:80/cgi-bin/capservice.

HTTP Port – Enter the HTTP or HTTPS port for the server. This will normally be port 80 for HTTP, or port 443 for HTTPS.

Username – Enter the username to login to the HTTP service. If this field is left blank, the login information will not be included in the communications.

Password – Enter the password to login to the HTTP service. If this field is left blank, the login information will not be included in the communications.

Confirm Password – Enter the password again for verification.

Audio Settings

Audio File Type – The audio file format is configurable as WAV or MP3.

Sample Rate – Select the sample rate for the audio files.

Sample Size – This setting is only available if the audio type is WAV. The audio sample size can be set to 8-bit or 16-bit.

Bit Rate – This setting is only available if the audio type is MP3. Select the bit rate of the audio. The default bit rate is 96kbps.

Audio Resource URL – This setting is used to construct the CAP message audio resource URI. The CAP message audio resource URI is constructed by appending the audio filename to the text that is configured here.

EAN Audio Option – An EAN is different from other EAS messages in that the audio can last indefinitely. For this reason, the EAN alert audio cannot be delivered as a file. This setting provides the following options for handling the EAN audio.

Do Not Include EAN Audio – There will not be an audio file delivered with the EAN nor will there be an audio resource in the CAP message. This is the default.

Deliver EAN FSK Audio – An audio file that only contains the EAS FSK and Attention tone will be delivered, and the CAP message will include an audio resource URI referencing this file. This can be useful for systems that force-tune to another channel to handle the EAN, but due to synchronization difficulties, can't guarantee that the EAS tones will be heard after the force-tune.

Include Audio Stream Resource URL – The CAP message will include the EAN Audio Stream URL (described below) as the audio resource. The audio stream referenced must be supplied by the system or reference a known EAN audio source.

EAN Audio Stream Resource URL – This setting is only available if the EAN Audio Option is set to "Include EAN Audio Stream URL". In this case, the text configured here will be used for the CAP message audio resource URI when an EAN is sent.

Do not deliver weekly tests that are received from a CAP source – Select this option to prevent required weekly tests that were received from CAP sources from being delivered to the selected server.

Remove State codes from weekly tests – Select this option to remove all State codes from the message before delivering it to the selected server. If there are no location codes left after removing the State codes, the message will not be delivered. The audio and display text will not be altered. If a state code is removed from the message, the display text will still show the state, and the EAS audio FSK will still include the state FIPS code.

Do not deliver monthly tests (RMT) – Select this option to prevent required monthly tests (RMT) from being delivered to the selected server.

Do not deliver Emergency Action Notifications (EAN) – Select this option to prevent Emergency Action Notifications (EAN) from being delivered to the selected server.

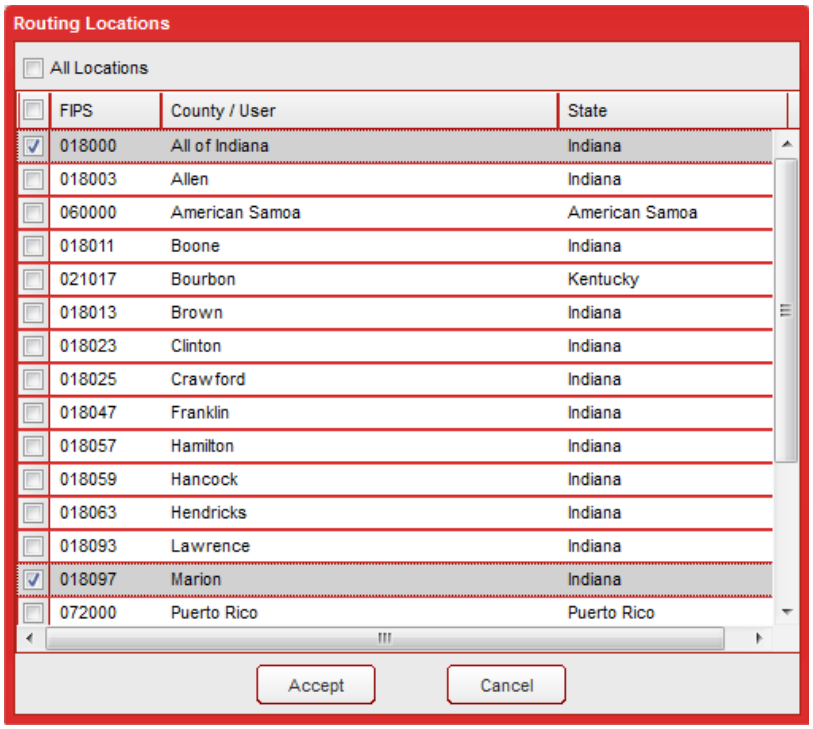
Do not deliver locally generated messages – Select this option to prevent messages that are generated locally (by an operator) from being delivered to the selected server.

source contains address – Include the IP address of the EASyCAP (and EASyPLUS) that received the message in the <source> element of the CAP message.

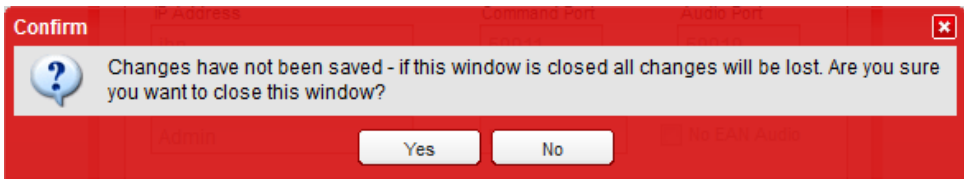
sender contains address – Include the IP address of the EASyCAP (and EASyPLUS) that received the message in the <sender> element of the CAP message.

Routing Locations – Click this button to open the **Routing Locations** page. This provides a method to configure the applicable locations for each server. Messages will only be delivered to the selected server if they contain one of the configured locations. Select the locations that are serviced by the selected server, or select All Locations to deliver all messages to the selected server.

Click **Accept** to save changes to the Routing Locations configuration or click **Cancel** to exit the **Routing Locations** page without saving changes.

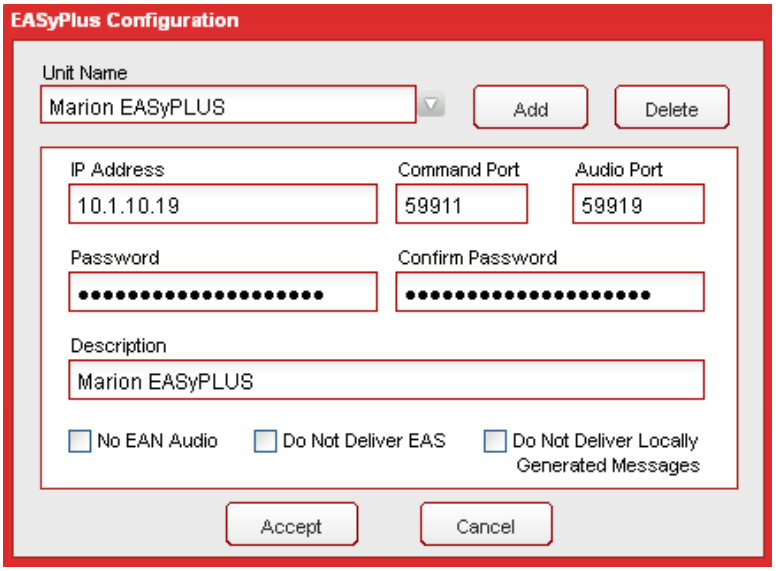


Select the **Accept** button to save your changes or the **Cancel** button to exit without saving any changes. If changes were made and the **Cancel** button is pressed, a confirmation page is displayed. Select the **No** button to return to the configuration page or select the **Yes** button to exit without saving changes.



EASyPLUS

To setup the delivery of CAP and EAS messages to EASyPLUS, EASyCAST, and EASyIPTV Encoder/Decoders, select the **EASyPLUS** link in the **Message Delivery** folder.



Unit Name – Select an EASyPLUS recipient from the drop-down menu to view and edit its settings.

Add button - Add a new EASyPLUS recipient.

Delete button - Delete the selected EASyPLUS.

IP Address – Enter the IP address of the selected EASyPLUS.

Command Port – Enter the TCP command port used to communicate with the selected EASyPLUS. The default value is 59911.

Audio Port – Enter the TCP port used to transfer audio to the EASyPLUS. The default value is 59919.

Password – Enter the password used to login to the EASyPLUS. This should be a special CAP account added to the user accounts of the EASyPLUS, and given EAS Alert and Ethernet permissions in the user account.

Confirm Password – Enter the password again for verification.

Description – Enter the name that you wish to display for this EASyPLUS.

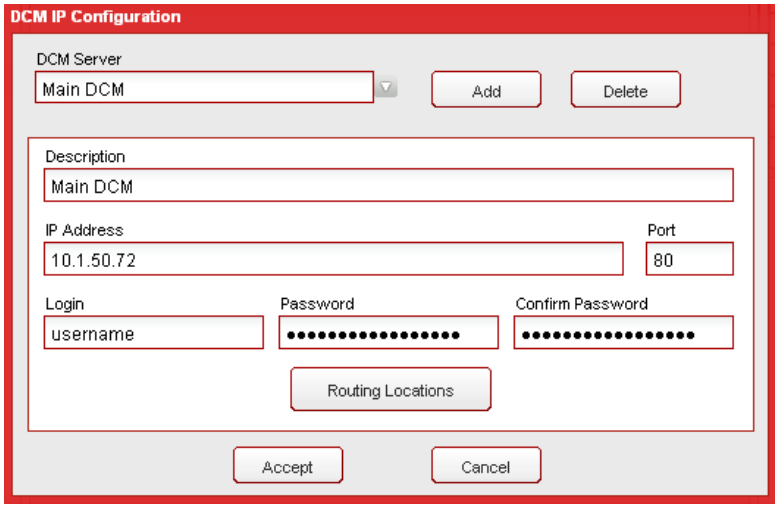
No EAN Audio – When this box is selected the EAN audio stream will not be used, the EASyPLUS will receive EAN audio from a local audio input.

Do Not Deliver EAS – When this box is selected, EAS messages received from EAS monitoring inputs will not be delivered to the selected EASyPLUS.

Do Not Deliver Locally Generated Messages – When this box is selected, messages that are generated locally will not be delivered to the selected EASyPLUS.

Select the **Accept** button to save your changes or the **Cancel** button to exit without saving any changes.

DCM



To configure DCM recipients, select the **DCM** link in the **Message Delivery** folder.

DCM Server – Select a DCM Server from the dropdown menu.

> **Add button** - Add a new DCM Server.
>
> **Delete button** - Delete the selected DCM server.

Description – Enter a descriptive name for the selected DCM Server.

IP Address – Enter the IP address of the DCM server.

Port – Select the TCP port used to communicate with the DCM server. The default port is 80.

Login – Enter the login username for the server.

Password – Enter the password for the server.

Confirm Password – Enter the password again for verification.

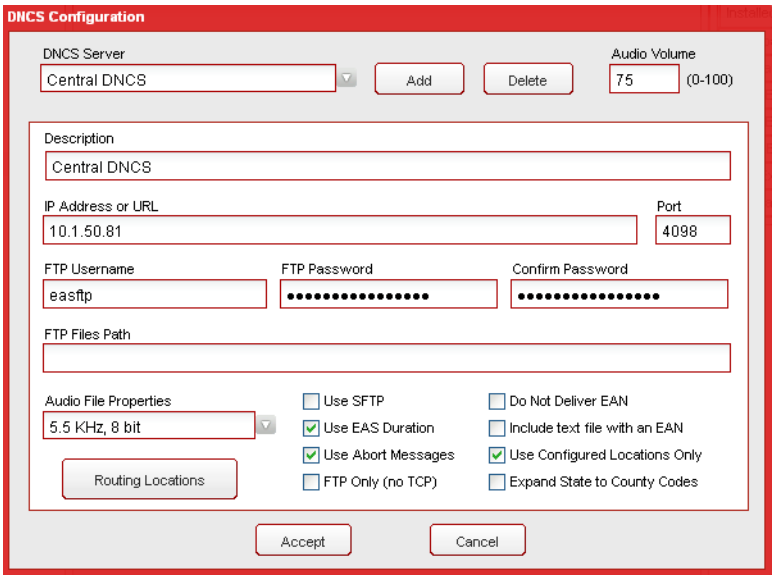
Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced. Select the locations that are serviced by the DCM server or select All Locations to disable location routing and deliver all messages to the selected device.

> Click **Accept** to save changes to the Routing Locations configuration or click **Cancel** to exit the **Routing Locations** window without saving changes.

Click **Accept** to save your changes or click **Cancel** to exit the without saving changes.

DNCS/Evertz

To configure message delivery to DNCS/Evertz devices, select the **DNCS/Evertz** link in the **Message Delivery** folder.



DNCS Server – Select the server from the dropdown menu.

> **Add button** – Add a new DNCS Server.
>
> **Delete button** – Delete the selected DNCS server.
>
> **Audio Volume** - Set the audio file volume (0-100).

Description – Enter the name to display for this DNCS Server.

IP Address or URL – Enter the IP Address or URL of the DNCS Server.

Port – Enter the TCP port of the DNCS. The default port is 4098.

FTP Username – enter the username required to login to the FTP server.

FTP Password – enter the password required to login to the FTP server.

Confirm Password – enter the password again for verification.

FTP Files Path – if different from the root path, enter the path where files need to be transferred.

Audio File Properties – Select the audio file properties from the dropdown menu. The default is 5.5kHz, 8bit.

Use SFTP – Select this option to use a secure SFTP server rather than an FTP server.

Use EAS Duration – Select this option to include the EAS duration in the socket message. A value of zero will be used for the duration if this option is not selected.

Use Abort Messages – Select this option to allow the EASyCAP® to deliver an EOM message when an operator manually aborts a message. Using the EOM as an abort message is not an official part of the specification and may not be supported by all devices.

FTP Only (no TCP) – Select this option to prevent the TCP socket message from being sent so only the audio and text files are transferred. This could be used for archiving systems or equipment that only needs the audio and text files. Do not select this option when delivering messages to a DNCS

Do Not Deliver EAN – Select this option to prevent EAN messages from being delivered to the selected DNCS/Evertz server.

Include text file with an EAN – Select this option to include the alert text file with an EAN event. Normally an EAN causes a force-tune and the text is not needed.

Use Configured Locations Only – Select this option to include only those areas configured in the Selected Locations screen.

Expand State to County Codes – Select this option to expand state-wide location codes into the configured county codes within the state. Note that the decision to send (or not send) messages based on routing locations is made prior to expanding state codes.

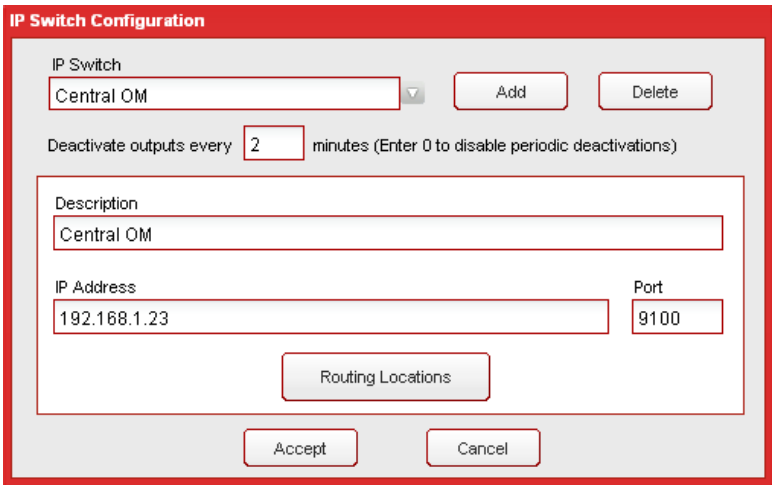
Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the server. Select the locations that are serviced by the DNCS server or select All Locations to disable location routing and deliver all messages to the selected server.

Click **Accept** to save the location selections or click **Cancel** to exit the **Routing Locations** window without saving locations selections.

Click **Accept** to save changes the configuration or click **Cancel** to exit the window without saving changes.

IP Switches

To configure IP Switches, select **IP Switches** in the **Message Delivery** folder.



IP Switch – Select an IP Switch from the dropdown menu.

Add – Add a new IP Switch.

Delete – Delete the selected IP Switch.

Deactivate outputs every <*n*> minutes – Enter the number of minutes to wait between (periodically) deactivating the outputs on all configured IP switches. Enter zero (0) to disable periodic deactivations.

Description – Enter the name to display for this IP Switch.

IP Address – Enter the IP address of the IP Switch.

Port – Enter the TCP Port number which is used to communicate with the IP switch (the default setting is 9100).

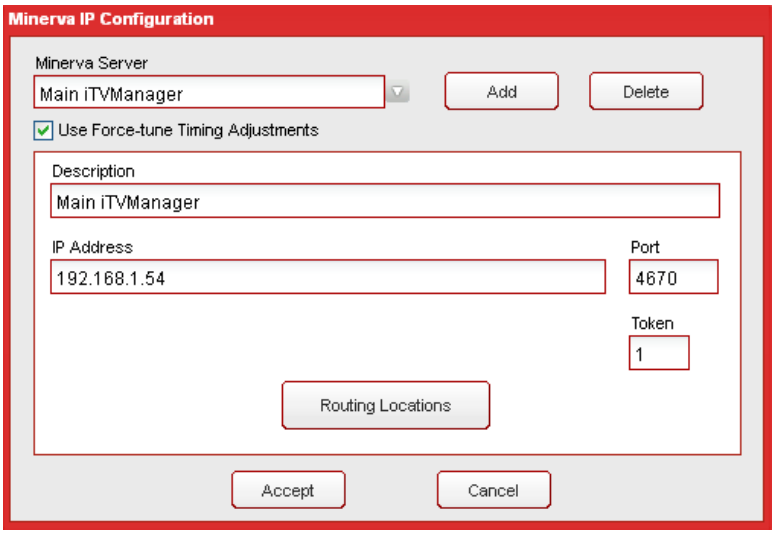
Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the switch.

Select the locations that are affected by the IP switch or select All Locations to disable location routing and deliver all messages to the selected switch. Click **Accept** to save the location selections or click **Cancel** to exit the **Routing Locations** window without saving locations selections.

Click **Accept** to save your changes or click **Cancel** to exit the **IP Switches** window without saving changes.

Minerva Configuration

To configure message delivery to Minerva servers, select **Minerva** in the **Message Delivery** folder.



Minerva Server – Select the server from the dropdown menu.

Add button – Add a new Minerva server.

Delete button – Delete the selected Minerva server.

Use Force-tune Timing Adjustments – Select this option to use the force-tune time adjustments (from the Playback Options screen) for messages delivered to Minerva servers.

Description – Enter the name to display for this Minerva Server.

IP Address – Enter the IP address of the Minerva Server in this field.

Port – Enter the TCP port used to communicate with the Minerva server (default port number is 4670).

Token – Enter the "token" for the EASyCAP® into this field. The "token" is used by the Minerva server to determine which Encoder/Decoder sent the message. The default is 1.

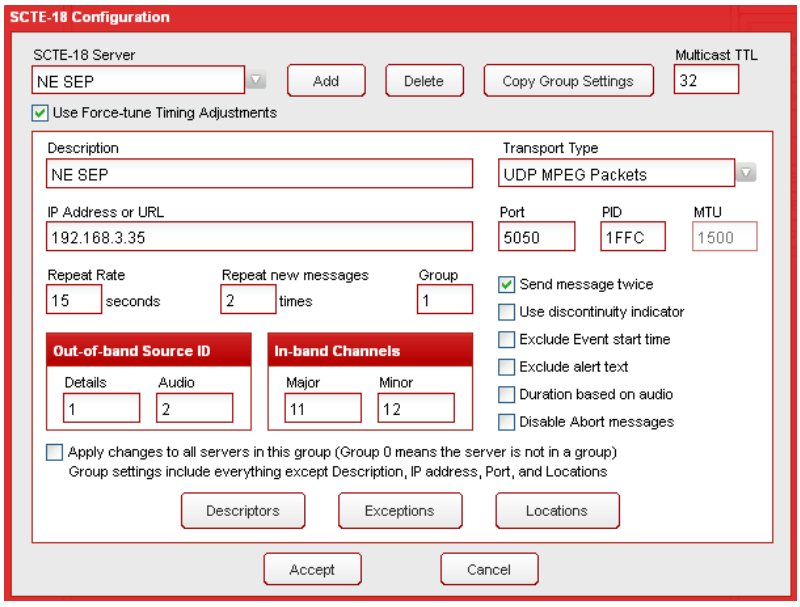
Routing Locations – Click this button to open the **Routing Locations** window.

The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the device. Select the locations that are affected by the server or select All Locations to disable location routing and deliver all messages to the selected server. Click **Accept** to save the location selections or click **Cancel** to exit the **Routing Locations** window without saving locations.

Click **Accept** to save your changes or click **Cancel** to exit the window without saving changes.

SCTE-18 Configuration

To configure SCTE-18 devices, select **SCTE-18** in the **Message Delivery** folder.



SCTE-18 Server – Select the SCTE-18 device from the dropdown menu.

Add button – Add a new SCTE-18 device.

Delete button – Delete the selected SCTE-18 device.

Copy Group Settings – Copies settings from the group to the selected SCTE-18 device. Make sure the correct group is selected in the Group edit box before copying settings.

Use Force-tune Timing Adjustments – Select this option to use the force-tune time adjustments (from the Playback Options screen) for SCTE-18 messages.

Multicast TTL – Enter the Multicast TTL for SCTE-18 messages.

Description – Enter the name to display for this device.

Transport Type – Select the digital transport protocol used to deliver SCTE-18 messages to the selected device.

NOTE

Vecima uses UDP MPEG packets but it's listed as a separate transport type because it requires a special sequence. If Vecima is selected but the Vecima Descriptor is not configured, the transport type will revert back to MPEG UDP Packets when the configuration changes are saved.

IP Address or URL – Enter the IP address or URL of the selected device.

Port – Enter the UDP port number for the selected device (default UDP port is 5050).

PID – Enter the PID for SCTE-18 messages delivered to this device. The PID is not used if the Transport Type is set to DOCSIS Set-top Gateway. The default PID for in-band devices is 1FFB, the default PID for out-of-band devices is 1FFC.

MTU – Enter the MTU for SCTE-18 messages delivered to this device. The MTU is only used for devices with the Transport Type set to DOCSIS Set-top Gateway. The default MTU is 1500.

Repeat Rate – Enter the interval for repeating SCTE-18 messages. Repeated messages are exact duplicates - the MPEG continuity_counter and SCTE-18 sequence_number will not be incremented. Repeats are used to guarantee devices receive the message and for devices that come online after the initial message was delivered. Messages will not be repeated if this is set to zero.

Repeat new messages – Enter the number of times to repeat the initial SCTE-18 message in order to establish an MPEG stream. The MPEG continuity_counter will be incremented for each packet sent.

Group – Enter a Group number (0-64) for the selected SCTE-18 Device, where a value of zero means the device is not included in any group. SCTE-18 Groups are provided to simplify the configuration process by allowing you to associate several SCTE-18 devices so that their configuration can be managed as a group. Assign the same Group number to devices that will be configured similarly. Then you can apply configuration changes to all of the devices in a group, or import settings from a group into a device. The group settings include all configuration except the device Description, IP address, port, and locations.

Out-of-band Source ID – Enter the out-of-band source information for the EAS Details Channel and Audio.

In-band Channels – Enter the Major and Minor Channel that represent the virtual channel number of the EAS Details channel. This only applies to in-band SCTE-18 messages. The system operator is responsible for providing PSIP support for the EAS Details channel.

Send Message Twice – Select this option to send the alert to the SCTE-18 device twice, incrementing the sequence_number on the second delivery. This helps to insure that the devices do not discard the alert due to a duplicate sequence_number.

Used discontinuity indicator – Select this option to include a discontinuity indicator at the beginning of each SCTE-18 transmission.

Exclude Event start time – Select this option to set the SCTE-18 event start time field to zero.

Exclude alert text – Select this option to prevent the alert text from being included in the SCTE-18 message.

Duration based on audio – Select this option to base the alert message time remaining on the length of the audio. If this is not selected, the alert message time remaining will be based on the length of the audio and video crawl, whichever is longer.

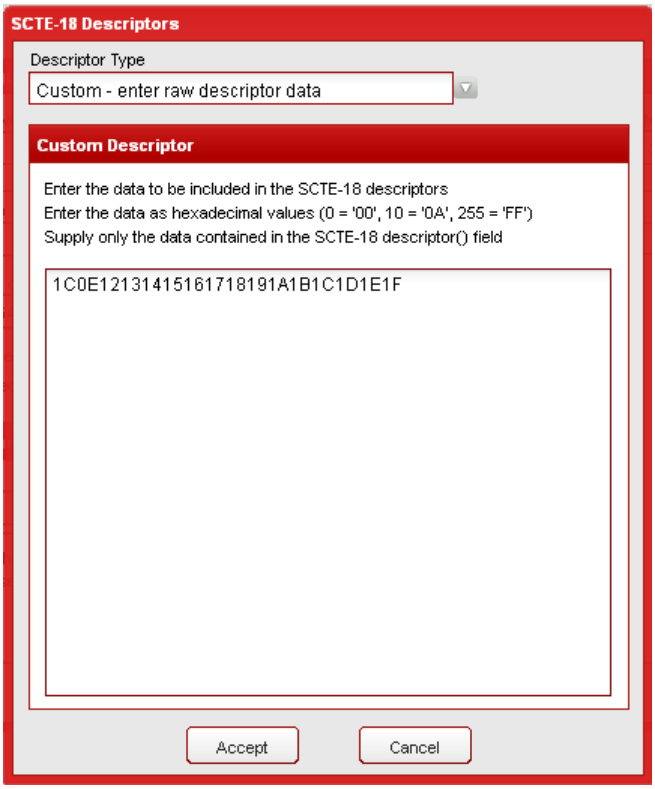
Disable Abort messages – Select this option to prevent abort messages from being sent to the device when an operator manually aborts a message.

Apply changes to all servers in the group – When checked, changes to the configuration will be saved to all devices in the group.

Descriptors - Click this button to open the **SCTE-18 Descriptors** window.

Descriptor Type – Select the type of descriptor from the dropdown menu.

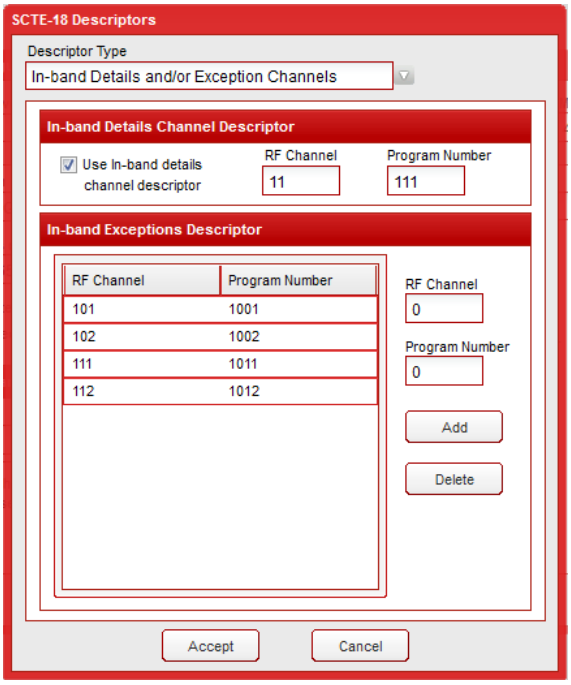
Custom Descriptor – The custom descriptor type is provided to enter descriptors not defined or supported in the GUI. When entering a custom descriptor you must enter the raw binary data that goes into the descriptor. The data is entered as hexadecimal values. All of the descriptor data, including the descriptor_tag and descriptor_length, must be included.

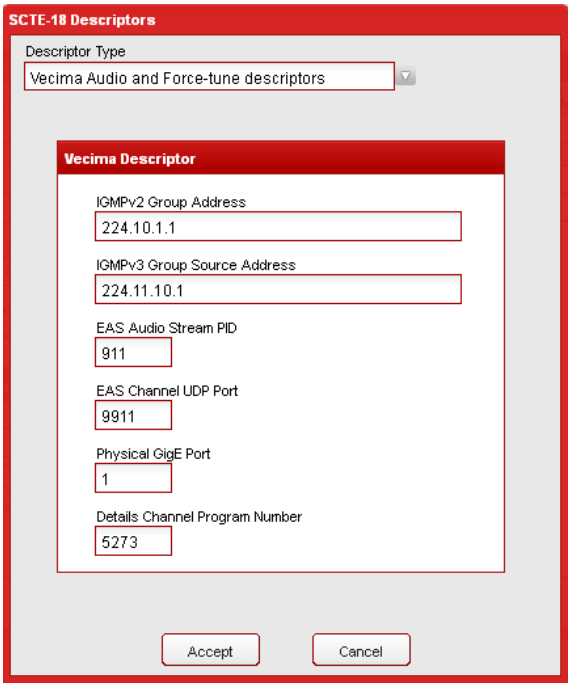


In-band Details Channel Descriptor – Click this checkbox if you want to use the in-band details channel descriptor. Enter the **RF Channel** and the **Program Number**.

In-band Exceptions Descriptor – In this box is a table of RF Channels and the associated Program Numbers. To add a new entry to the table, enter the **RF Channel** and the **Program Number**, then click **Add**. To delete an entry, click the item in the table you want to delete so it is highlighted, then click **Delete**.

Vecima Audio & Force-tune Descriptor – The Vecima descriptor is used to inform the CableVista where to find the EAS Details MPEG stream. The Vecima descriptor cannot be used if the Transport Type is set to DOCSIS Set-top Gateway.





IGMPv2 Group Address – Enter the IGMP version 2 group multicast address.

IGMPv3 Group Source Address – Enter the IGMP version 3 group source multicast address.

EAS Audio Stream PID – Enter the PID for the EAS audio stream (16-8190).

EAS Channel UDP port – Enter the UDP port for the EAS Details channel (256-65535).

Physical GigE Port – Enter the physical GigE port used (1 or 2).

Details Channel Program Number – Enter the program number for the EAS Details channel (1-65535).

Click **Accept** to save changes to the descriptor or click **Cancel** to exit the **SCTE-18 Descriptors** window without saving selections.

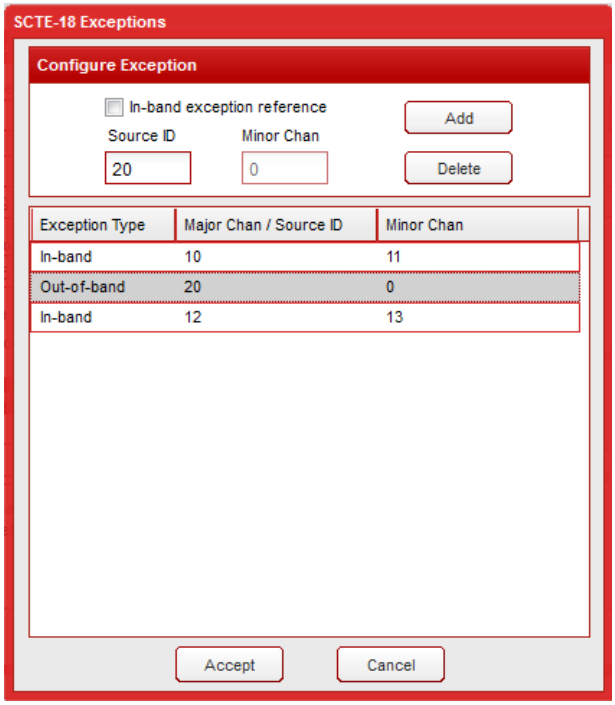
Exceptions – Click this button to open the **SCTE-18 Exceptions** window.

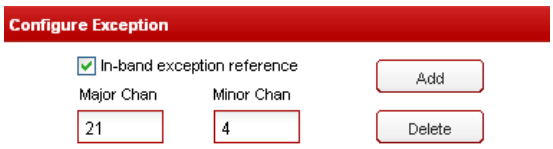
Add an exception – Enter the Source ID and press the Add button (Minor Channel is not used).

Add an in-band exception – Check the In-band exception reference, enter the Major and Minor channel numbers, and then press the Add button.

Delete an exception – Click the exception in the list that you want to delete so it is highlighted, then press the Delete button.

Click **Accept** to save changes to the exceptions or click **Cancel** to exit the **SCTE-18 Exceptions** window without saving selections.

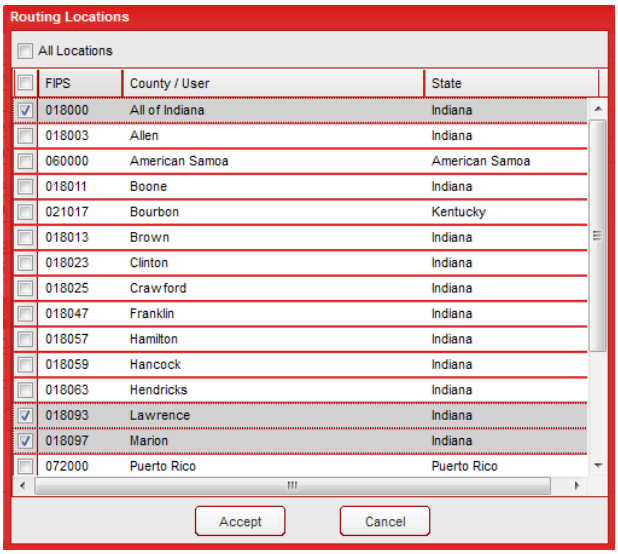




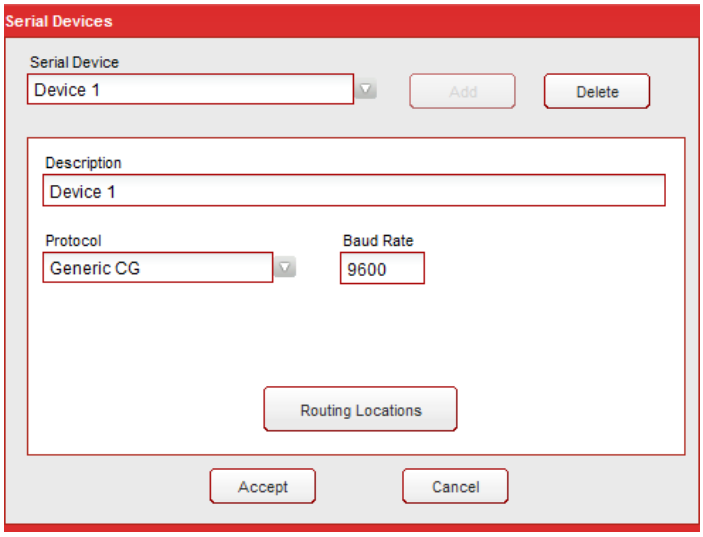
Routing Locations – Click this button to open the **Routing Locations** window. The routing locations allow each device to serve a different geographical location, and to prevent unnecessary interruption if the alert message is not intended for the locations serviced by the device.

Select the locations that are affected by the device or select All Locations to disable location routing and deliver all messages to the selected device.

Click **Accept** to save the selected routing locations or click **Cancel** to exit the **Routing Locations** window without saving the selected locations.



Serial Devices



To configure Serial Devices, select **Serial Devices** in the **Message Delivery** folder. The **Serial Devices** window will be displayed.

Serial Device – Select the type of serial device from the dropdown menu.

Add – Add a new serial device.

Delete – Delete the selected serial device.

Description – Enter a name to display for this Serial Device.

Protocol – Select the protocol used to communicate with the device from the dropdown menu. The Chyron and Star-8 CG protocols provide configuration for the Crawl Position and number of Crawl Repeats. Chyron protocol also allows the Crawl Speed to be configured.

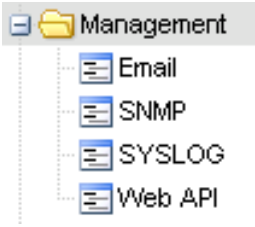
Baud Rate – Enter the serial baud rate.

Routing Locations – Click this button to open the **Routing Locations** window. Click the checkboxes to select locations and areas. Click **Accept** to save the selected locations or click **Cancel** to exit the **Routing Locations** window without saving the selected locations.

Click **Accept** to save your changes or click **Cancel** to exit the window without saving changes.

Management Folder

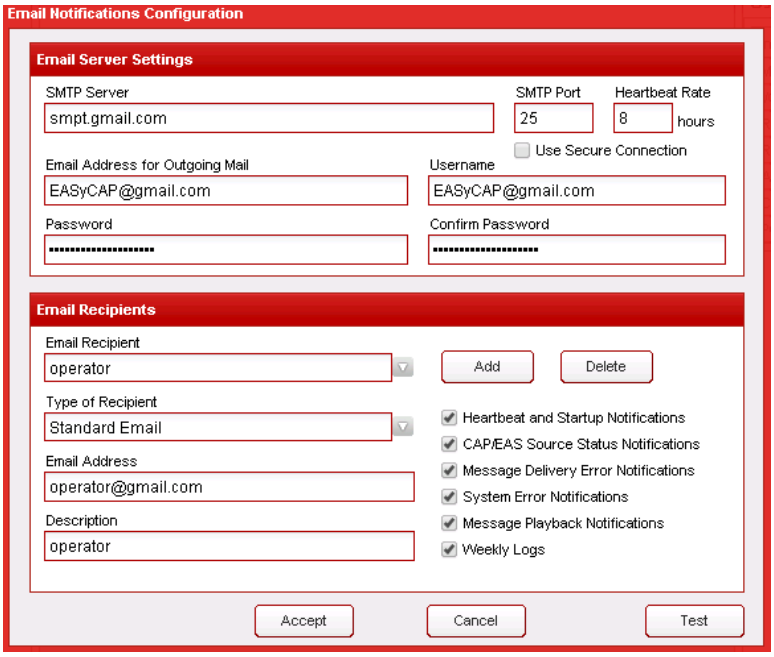
Expand the **Management** folder in the Navigation bar by clicking the **+** sign next to the folder.



Email

This feature provides the ability to deliver Email notifications to a list of recipients. The Email feature requires an Email License or a Network Management License.

To view or configure Email, select the **Email** link from the **Management** folder.



Email Server Settings -

SMTP Server – Enter the SMTP server URL.

SMTP Port – Enter the SMTP port (default is 25).

Email Address for Outgoing Mail – Enter the Email address used for outgoing mail.

Use Secure Connection – When enabled, a secure connection will be used when the SMTP server reports that it supports TLS.

Heartbeat Rate – Enter the number of hours between heartbeat Emails.

Username – Enter the username required to login to the SMTP server.

Password – Enter the password required to login to the SMTP server.

Confirm Password – Enter the password again for verification.

Email Recipients -

Email Recipient – Select the Email recipient to edit or view from the drop-down box.

Add – Add a new Email recipient.

Delete – Delete the selected Email recipient.

Type of Recipient – For normal Email recipients, select Standard Email, otherwise choose the appropriate SMS/MMS provider.

Email Address – Enter the Email address of the recipient. For SMS/MMS, enter the recipient's phone number, including area code.

Description – Enter a name to display for this Email recipient.

Heartbeat and Startup Notifications – Select this option to deliver heartbeat and startup Emails to the selected recipient.

CAP/EAS Source Status Notifications – Select this option to deliver an Email when the connection to a CAP source is lost, when an EAS source loses audio signal, or when an EAS source detects an audio signal.

Message Delivery Error Notifications – Select this option to send an Email when a message cannot be delivered to an external device (server, character generator, switch).

System Error Notifications – Select this option to send an Email when a system error occurs, for example when a critical process becomes unresponsive.

Message Playback Notifications – Select this option to send an Email when message playback begins.

Weekly Logs – Select this option to send an Email every Sunday at midnight containing the previous weeks logs.

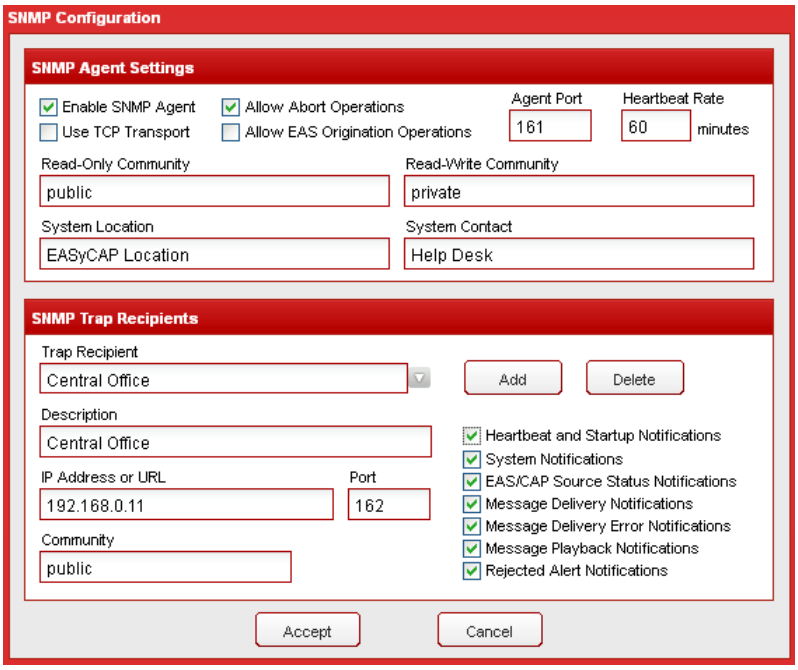
Press the **Test** button to send a test Email to all configured recipients.

Press the **Accept** button to save changes to the configuration or choose **Cancel** to exit without saving changes.

SNMP

The EASyCAP® SNMP feature is MIB-II (RFC 1213) compliant and supports the HOST-RESOURCES (RFC 2790) MIB, UCD-SNMP MIBs, and the EASyCAP® MIB. The SNMP feature requires a Network Management License.

To configure SNMP, select the **SNMP** link from the **Management** folder.



SNMP Agent Settings -

Enable SNMP Agent – Enable SNMP.

USE TCP Transport – Select this option to use a TCP transport for SNMP GET and SET operations. UDP is the recommended transport.

Allow Abort Operations – Select to allow users to Abort (and Confirm) messages via SNMP SET operations.

Allow EAS Origination Operations – Select to allow users to originate EAS messages via SNMP SET operations.

Agent Port – Enter the SNMP Agent port (default is 161).

Heartbeat Rate – Enter the number of minutes between heartbeat traps.

Read-Only Community – Enter the community string for read-only access.

Read-Write Community – Enter the community string for read and write access.

System Location – Enter the system location for the MIB-II system group.

System Contact – Enter the system contact for the MIB-II system group.

SNMP Trap Recipients -

Trap Recipient – Select the SNMP Trap recipient to edit or view.

Add – Add a new Trap recipient.

Delete – Delete the selected Trap recipient.

Description – Enter a name to display for the this Trap recipient.

IP Address or URL – Enter the IP address or URL for the selected Trap recipient.

Port – Enter the port use for sending SNMP Traps (default is 162).

Community – Enter the community string for Traps delivered to the selected recipient.

Heartbeat and Startup Notifications – Select this option to deliver heartbeat and startup Traps to the selected recipient.

System Notifications – Select this option to send system information and error Traps, for example when a user logs into the web server.

EAS/CAP Source Status Notifications – Select this option to deliver a Trap when the connection to a CAP source is lost, when an EAS source loses audio signal, and when an EAS source detects an audio signal.

Message Delivery Notifications – Select this option to send a Trap when a message is successfully delivered to an external device (server, character generator, switch).

Message Delivery Error Notifications – Select this option to send a Trap when a message cannot be delivered to an external device (server, character generator, switch).

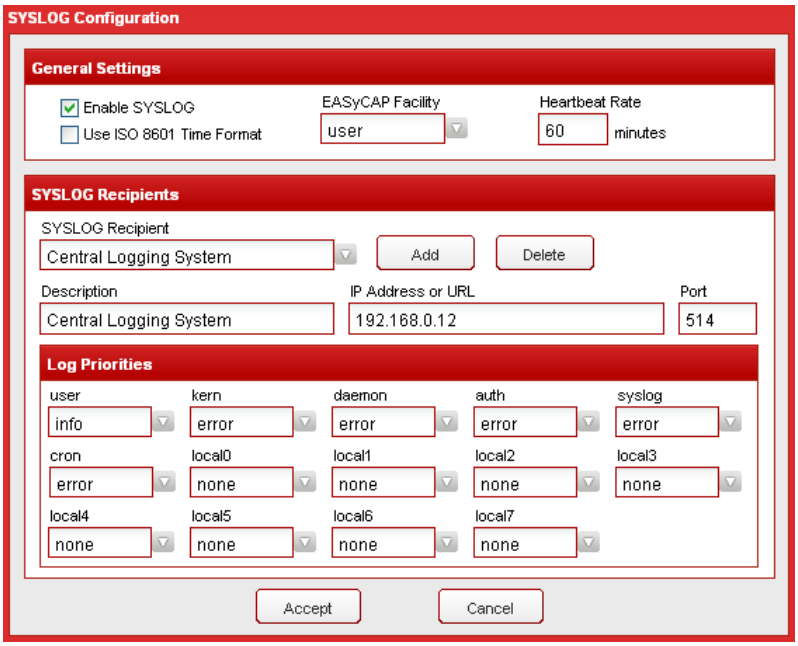
Message Playback Notifications – Select this option to send an EMail when message playback begins.

Rejected Alert Notifications – Select this option to send a Trap when a received alert message is rejected.

Press the **Accept** button to save changes to the configuration or choose **Cancel** to exit without saving changes.

SYSLOG

The SYSLOG feature adds the ability to send syslog messages to remote servers for monitoring and centralized logging. Syslog cannot be used for the EAS log required by the FCC. A Network Management License is required.



General Settings -

Enable SYSLOG – Enable SYSLOG to send syslog logs to the configured recipients.

USE ISO-8601 Time Format – Select this option to use the ISO-8601 date/time format for the logs (for example 2013-07-22T12:07:25.079487-04:00). Make sure that your syslog client supports this format before selecting this option. The standard syslog time format is used by default.

EASyCAP Facility – Select the facility that the EASyCAP® software uses when sending syslog messages.

Heartbeat Rate – Enter the number of minutes between heartbeat messages.

SYSLOG Recipients -

SYSLOG Recipient – Select the SYSLOG recipient to edit or view.

Add – Add a new SYSLOG recipient.

Delete – Delete the selected SYSLOG recipient.

Description – Enter a name to display for the this SYSLOG recipient.

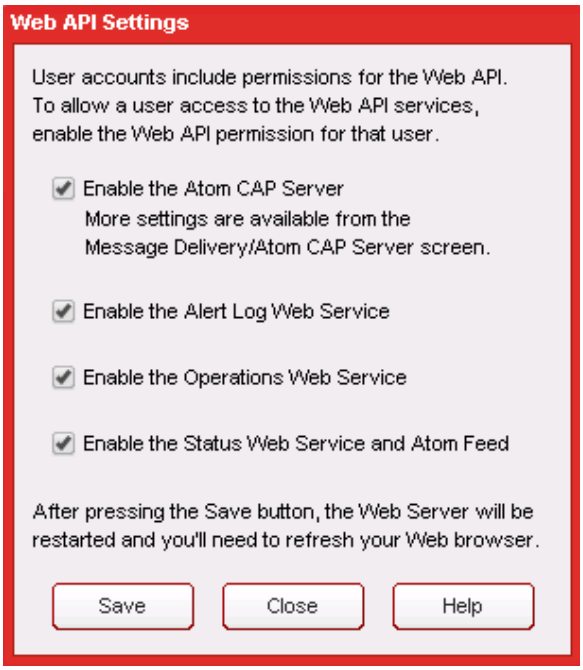
IP Address or URL – Enter the IP address or URL for the selected SYSLOG recipient.

Port – Enter the port used for sending SYSLOG messages (default is 514).

Log Priorities – Set the desired log priority for each syslog facility. Log messages with the configured priority and higher will be delivered to the recipient. Set the priority to **none** to disable logs for that facility.

Press **Accept** to save configuration changes or choose **Cancel** to exit without saving.

Web API



The Web API feature provides interfaces to several Web Services and Atom feeds. An Atom CAP Server or Network Management license is required. Note that a user account must be configured with permission to use the **Web API** and the Web Service clients must use these login credentials. For details on available Web Services see the EASyCAP® Web API document, or press the **Help** button.

Enable the Atom CAP Server – Enable the **Atom CAP Server** to provide an IPAWS Open style Atom feed that includes all received EAS, CAP, and locally generated messages. Requires an Atom CAP Server license.

Enable the Alert Log Web Service – When enabled, a Web Service is available to allow https clients to retrieve logs in text and JSON format. Requires a Network Management license.

Enable the Operations Web Service – When enabled, a Web Service is available to allow https clients to perform operations like aborting a message in progress or confirming a pending message. Requires a Network Management license.

Enable the Status Web Service and Atom Feed – When enabled, a Web Service is available to https clients to retrieve status information about message activations and CAP/EAS sources. An Atom feed is also provided, allowing any standard RSS or Atom feed software to be used to monitor the status of message activations and CAP/EAS sources. Requires a Network Management license.

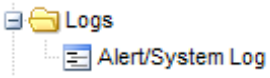
Press the **Save** button to save any configuration changes. You may need to refresh your Web Browser after pressing **Save** because the Web Server was restarted.

Press the **Close** button to exit the Web API Settings window.

Press the **Help** button to view the EASyCAP® Web API document.

Logs

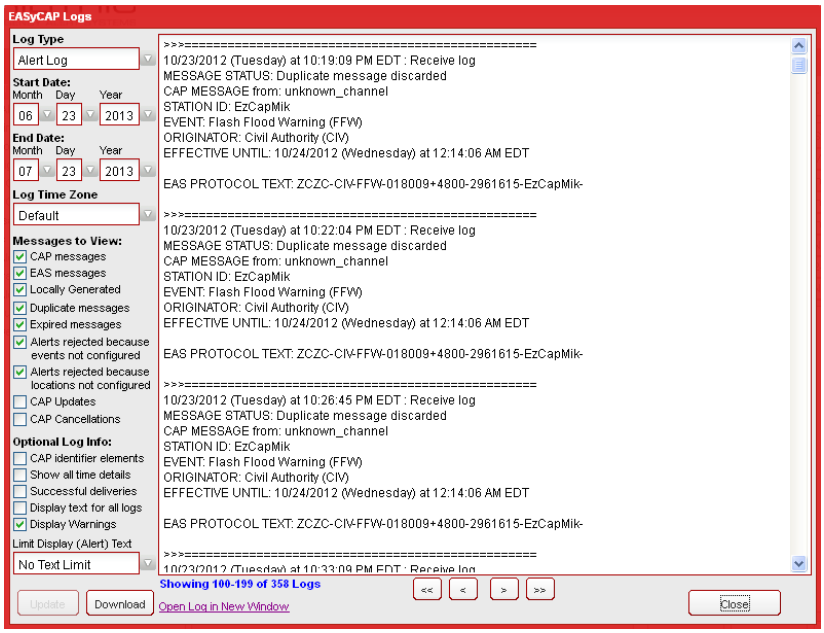
Expand the Logs folder in the Navigation bar by clicking the + sign next to the Logs folder.



Alert/ System Log

To view the alert and system logs of the EASyCAP®, select the **Alert/System Log** link in the **Logs** folder.

Alert Log



Select **Alert Log** from the **Log Type** drop-down list to view Alert information.

Set the time period of the log by selecting the **Start Date** and **End Date**. The **Log Time Zone** allows you to specify which time zone to use for the log, where **Default** is the time zone of the EASyCAP®.

Select the message types to included in the log by selecting the appropriate **Messages to View** check-boxes.

Select the type of information included in the log by selecting the desired **Optional Log Info** check-boxes.

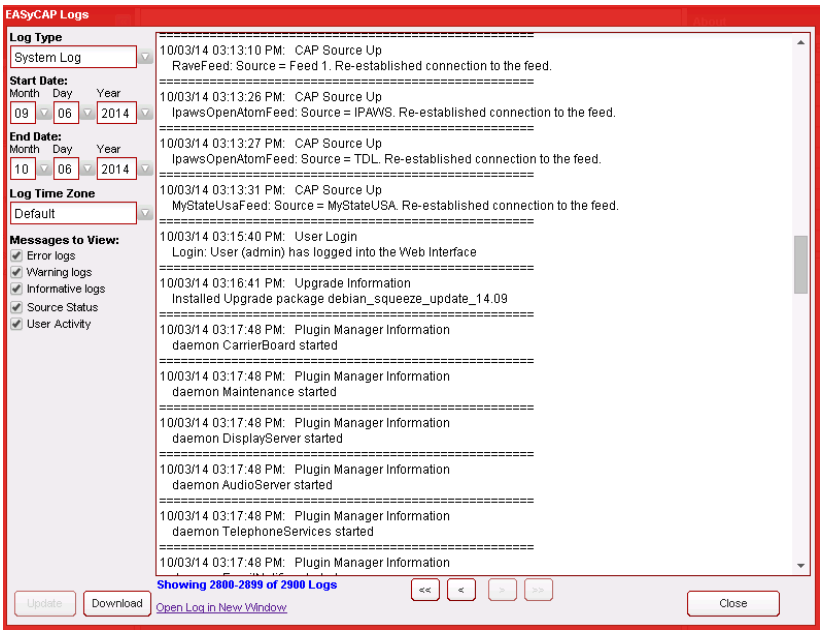
The length of the alert text in the logs can be limited by using the **Limit Display (Alert) Text** drop-down list.

Press the **Update** button to create and view the log. The alert log will be displayed as shown above. One hundred log records are displayed at a time. Use the **<<** (First), **<** (Previous), **>** (Next), and **>>** (Last) buttons to navigate through all of the log records.

Click the **Open Log in New Window** link to view the log text in a separate browser window.

Press the **Download** button to download a copy of the alert log as an ASCII text file.

System Log



Select **System Log** from the **Log Type** drop-down list to view general system and application information.

Set the time period of the log by selecting the **Start Date** and **End Date**. The **Log Time Zone** allows you to specify which time zone to use for the log, where **Default** is the time zone of the EASyCAP®.

Select the types of log records to include by selecting the appropriate **Messages to View** check-boxes.

Press the **Update** button to create and view the log. The system log will be displayed as shown.

One hundred log records are displayed at a time. Use the **<<** (First), **<** (Previous), **>** (Next), and **>>** (Last) buttons to navigate through all of the log records.

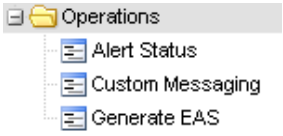
Click the **Open Log in New Window** link to view the log text in a separate browser window.

Press the **Download** button to download a copy of the system log as an ASCII text file.

Click **Close** to close the **EASyCAP Logs** screen.

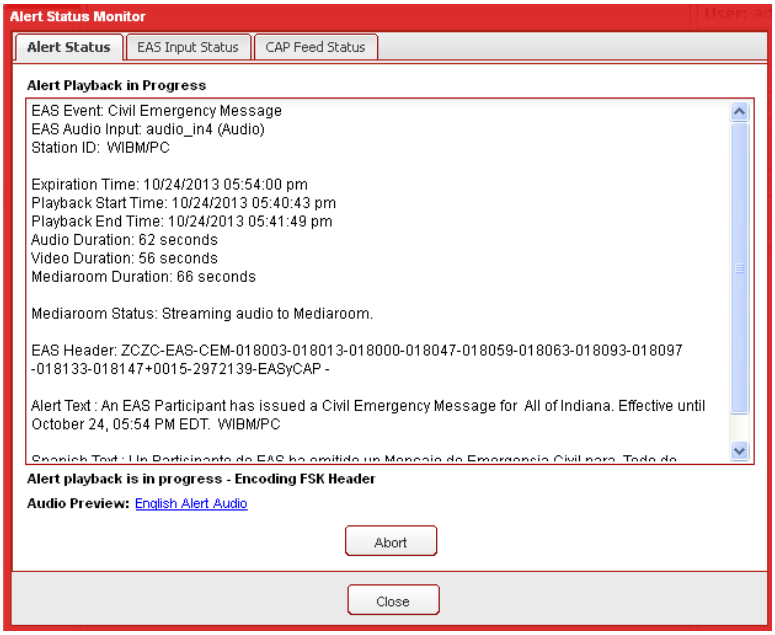
Operations

Expand the **Operations** folder in the Navigation bar by clicking the **+** sign next to the folder.



Alert Status Monitor

To view the Alert Status Monitor of the Encoder/Decoder, select **Alert Status** in the **Operations** folder. The **Alert Status Monitor** window will be displayed. This window has three tabs; Alert Status, EAS Input Status, and IPAWS Atom Feed Status.



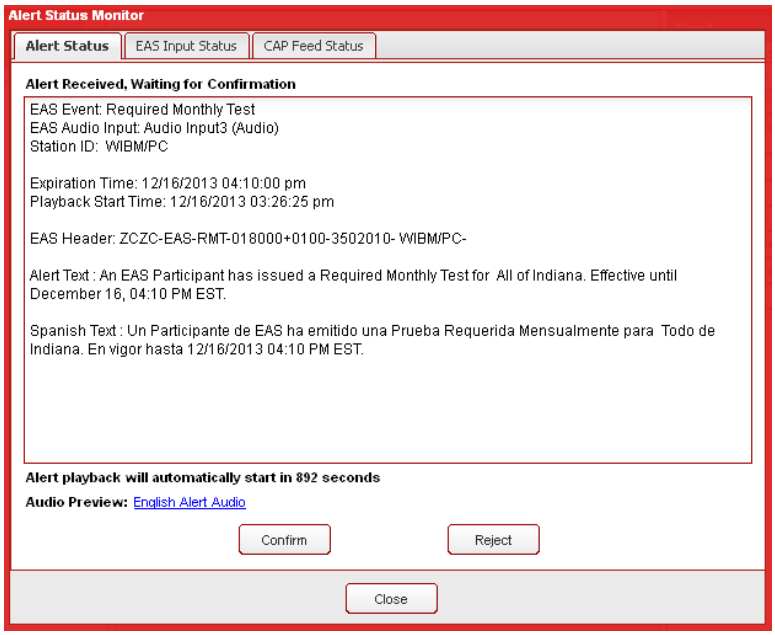
Alert Status Tab

The **Alert Status** screen provides the current status of EAS activations as well as a means to abort the current alert message. The status shown in your Web Browser is periodically updated. You can configure how often to update the status information by going to the **Web Services Configuration** screen and changing the value for the Status Timer.

During an EAS activation, the operator can view information about the alert in progress, including: EAS Event; EAS header text; expiration time; audio duration; and alert text.

An **Abort** button is provided to allow the operator to abort the alert that's in progress.

Broadcast Application in Manual Mode – The **Alert Status** screen allows Broadcast operators to preview the alert information and audio before the alert is aired. This is only applicable when in Manual mode and the EAS Event is configured with a delay. A countdown is displayed to show how much time is left before the alert is automatically aired. The audio can be previewed by clicking on the Audio Preview link near the bottom of the screen.

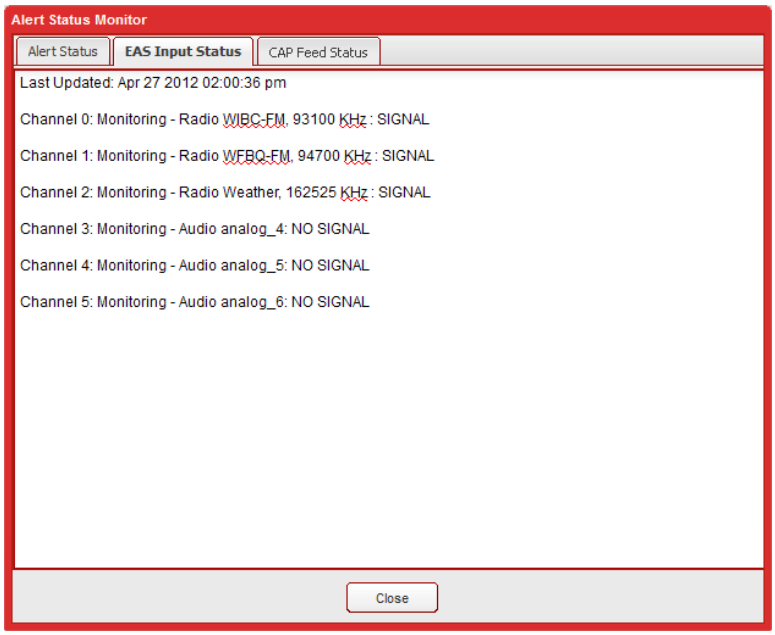


Click the **Confirm** button to confirm the alert and begin playback.

Click the **Reject** button to cancel the alert playback.

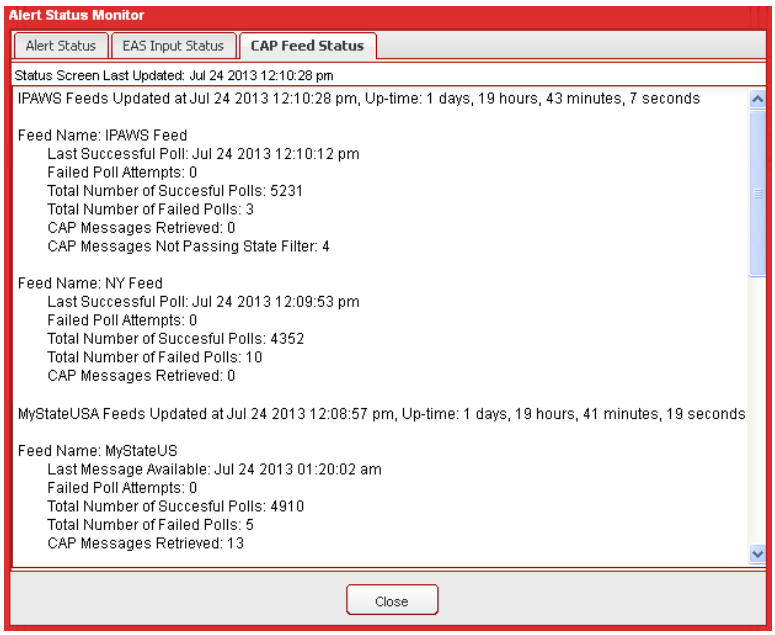
EAS Input Status Tab

The EAS Input Status tab displays the date and time that the Monitor was last updated and displays the status of each input channel. The same information shown on the front panel LCD can be viewed here.



CAP Feed Status Tab

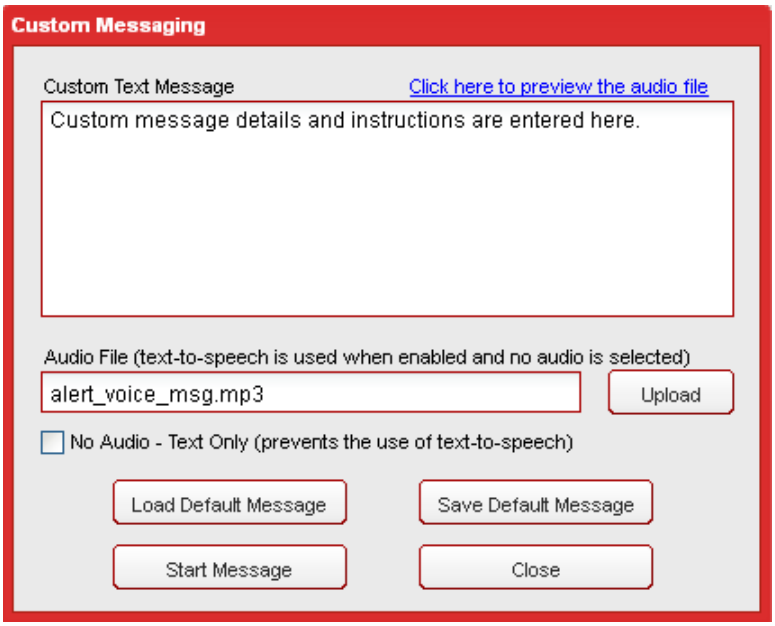
The CAP Feed Status tab displays the date and time that the Monitor was last updated and displays the status of each configured CAP feed.



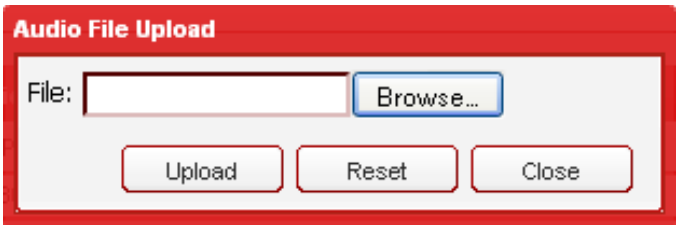
Click **Close** to close the **Alert Status Monitor** window.

Custom Messaging

To generate custom messages, click **Custom Messaging** in the **Operations** folder. The **Custom Messaging** window will appear.



- **Custom Text Message** - Enter a custom text message. The text is limited to 1750 characters. Do not use characters &, %, or /. Note that the EASyCAP® must be licensed for Custom Messaging.
- **Audio File** - Shows the audio file selected for the message.
- **Upload** - Upload an audio file for the message. Press the **Upload** button. The **Audio File Upload** window will be displayed. Press the **Browse** button to select an audio file and then press the **Upload** button. Click **Close** to exit the **Audio File Upload** window.



- **No Audio - Text Only** - Select this check-box to guarantee that audio is not played during the custom message. If text-to-speech is enabled, this option will prevent it from being generated.

Save Default Message - Press this button to save the custom text message and audio file that are currently loaded. These files are saved with your user account so that they can be loaded later. The default audio file can also be used when originating a message from a telephone.

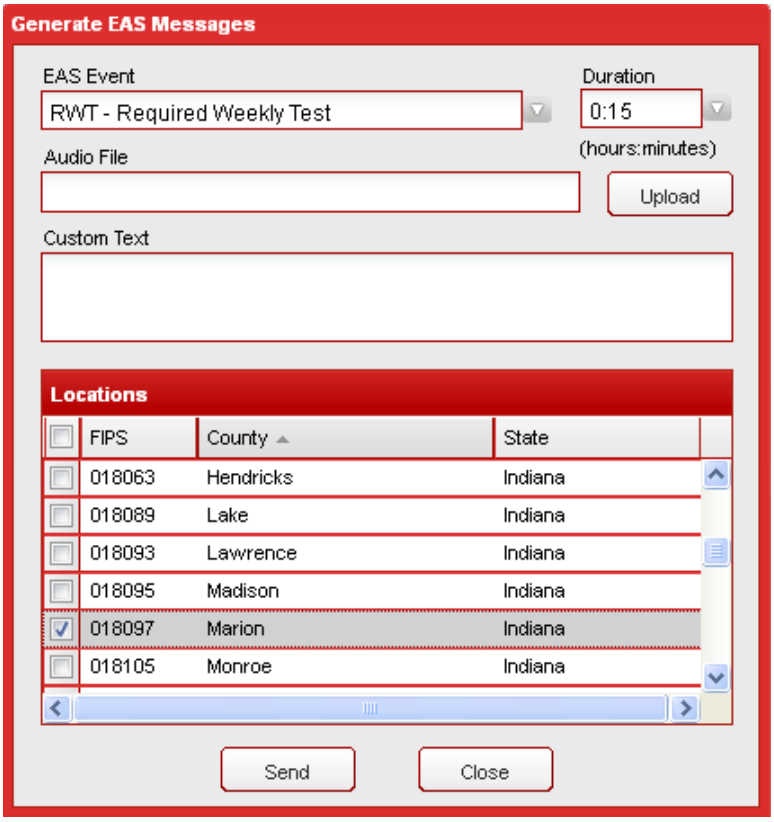
Load Default Message - Press this button to load the default custom text and audio that were previously saved.

The **Click here to preview audio file** link will appear when a valid audio file is loaded. Click this link to preview the audio in a separate browser window.

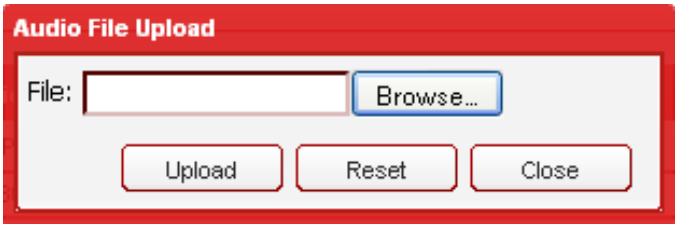
Press the **Start Message** button to start the custom message or press the **Close** button to exit the **Custom Messaging** window.

Generate EAS

To generate EAS messages, click **Generate EAS** in the **Operations** folder. The **Generate EAS Messages** window will appear.



- **EAS Event** - Select the EAS event that you want to generate from the dropdown menu.
- **Duration**- Enter the EAS duration for the message.
- **Audio File** - Shows the audio file selected for the message.
- **Upload** - Upload an audio file for the message. Press the **Upload** button. The **Audio File Upload** window will be displayed. Press the **Browse** button to select an audio file and then press the **Upload** button. Click **Close** to exit the **Audio File Upload** window.
- **Custom Text** - Enter custom text for the EAS message. The custom text will be appended to the normal EAS translation text. Do not use characters &, %, or /. Note that the EASyCAP® must be licensed for Custom Messaging before this option can be used.
- **Locations** - Click the checkboxes to select the locations that are included in the EAS message.



Press the **Send** button to generate the EAS message or press the **Close** button to exit the **Generate EAS Messages** window.

THIS PAGE INTENTIONALLY LEFT BLANK

Telephone Interface

The EASyCAP® Telephone Interface allows operators or emergency management personnel to activate and abort messages by dialing into an EASyCAP® Encoder/Decoder equipped with a Telephone interface option board. It can be used to generate EAS messages, custom (non-EAS) messages, and to abort messages in progress. Each user is assigned a personal identification number (PIN) by the EASyCAP® administrator. This PIN is required to authenticate telephone users. Each user is also assigned one or more location codes so that messages can be routed to specific areas based on the user that's logged in.

NOTE

These instructions provide too much detail to be used during an emergency. The EASyCAP administrator is encouraged to make a short instruction sheet for telephone users to follow. It should contain the telephone number, PIN (if allowed to be documented), and sequence of keys and prompts that will activate the EASyCAP.

User Prompts

Three tones are used by the EASyCAP® to provide feedback to the telephone user.

- **ACK** - A low to high tone indicating success or an accepted command
- **NACK** - A discordant high to low tone indicating rejection of a command
- **BEEP** - A 1 KHz tone used to prompt the user for a PIN, or to record a message

Command Keys

Command keys may be zero through nine, as well as

The pound key, used to enter a command (or the PIN)

***** The asterisk key, used to cancel a command sequence if a mistake is made

Operations

All operations are initiated by using a 2-digit command. The following lists the available operations:

- 00# Hang-up the Telephone
- 01# Abort the message in progress
- 02# Record and save a user audio message
- 10# Activate a custom (non-EAS) message
- 11# - 62# Activate an EAS message
  The 2-digit command corresponds to an EAS Event, see list below.

Dial-up and Authentication

To use the telephone interface, dial the number for the telephone line connected to the EASyCAP® and wait for the **BEEP** prompt. After the prompt, enter your (4 to 8 digit) PIN number followed by the **#** key.

- Dial the Telephone number for the EASyCAP
- Wait until Telephone is answered and a **BEEP** is heard
- Enter your PIN number followed by the **#** key

Once the **#** key is pressed, an **ACK** prompt will indicate a successful login, or a **NACK** prompt will indicate that the PIN is invalid or that user permissions are insufficient. Three attempts to enter the correct PIN are allowed before the EASyCAP® hangs up.

Hang-up Telephone

Always issue the hang-up command before hanging up the Telephone to guarantee that the EASyCAP's Telephone line is on-hook and it is ready to accept a new call.

To command the EASyCAP to hang-up the Telephone, enter **00** followed by the **#** key. The EASyCAP will play an **ACK** prompt and then hang up the Telephone.

- Enter **00** followed by the **#** key
- Wait until the **ACK** prompt is heard and the Telephone is hung up

Abort Message in Progress

To abort a message that's in progress, enter **01** followed by the **#** key.

- Enter **01** followed by the **#** key
- Wait until the **ACK** or **NACK** prompt is heard

An **ACK** prompt indicates that the message in progress was successfully aborted. A **NACK** prompt indicates that the message was not aborted. This is normally caused by the user account not having permission to abort messages from the Telephone.

Record User Audio Message

One default user audio message can be saved for each user. It is saved into permanent storage so that it can be quickly loaded and used for message activations. The audio message has a maximum duration of two minutes. Note that this is the same default audio message used by the Web Interface for custom messaging.

To record the user audio message, enter **02** followed by the **#** key.

- Enter **02** followed by the **#** key
- Wait until the **BEEP** prompt is heard, recording starts immediately after the prompt
  - If a **NACK** prompt is heard, the operation failed (normally because a message is in progress)
- Speak into the Telephone, a maximum of 2 minutes can be recorded
- Press the **#** key to stop recording audio
  - Press the * key to cancel the recording and delete the audio message
- Wait until the **ACK** prompt is heard

Activate a Custom (Non-EAS) Message

Custom (non-EAS) messages can be activated from the Telephone interface. The Web Interface provides the ability to save one default audio and one default text message for each user account. The default audio and text messages can be programmed and saved from the Web Interface's **Custom Messaging** page (go to the **Operations** folder and select the **Custom Messaging** link). This allows the operator to preload an audio and text message which can be activated later from the Telephone. If a default custom text message has not been saved, the text message displayed when a Custom Message is activated from the Telephone will be as follows: "A community access message is in progress. Listen to the audio on this channel for detailed information."

To activate a custom (non-EAS) message that uses audio recorded from the Telephone, enter **10** followed by the **#** key.

- Enter **10** followed by the **#** key
- Wait until the **BEEP** prompt is heard, recording starts immediately after the prompt
  - A **NACK** prompt is heard if the operation failed (because a message is in progress)
- Record the audio message by speaking into the Telephone (2 minutes maximum)
- Press the **#** key to stop recording audio
  - Press the * key to cancel the message activation and delete the audio
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

The command to activate a custom (non-EAS) message can optionally include an additional parameter to setup the type of audio used.

Audio Option (third digit of the command)

The user can optionally specify what type of audio is used for the message by entering a third digit in the command. This parameter is optional. If it's not included the message will default to using audio recorded from the Telephone.

- 0 Use audio recorded from the Telephone
  This is the default and is used if the audio option is not specified
- 1 Use the pre-recorded default user audio message
- 2 Use text-to-speech
  Note that this option only functions if the EASyCAP text-to-speech is enabled
- 3 No audio (text only)

To activate a custom (non-EAS) message that uses the pre-recorded default audio message, enter **101** followed by the **#** key.

- Enter **101** followed by the **#** key
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

To activate a custom message that uses text-to-speech, enter **102** followed by the **#** key.

- Enter **102** followed by the **#** key
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

To activate a text-only custom message that does not include audio, enter **103** followed by the **#** key.

- Enter **103** followed by the **#** key
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

Activate EAS Message

EAS messages can be activated from the Telephone interface. A two-digit command is provided for each EAS Event code (see list below). Two additional digits can be optionally included to select the audio type and message duration. The user's configured locations determine which FIPS codes are included in the EAS message.

EAS Message Commands (first two digits of the command)

- 11 Required Monthly Test
- 12 Required Weekly Test
- 13 Administrative Message
- 14 Avalanche Watch
- 15 Avalanche Warning
- 16 Blizzard Warning
- 17 Child Abduction Emergency
- 18 Civil Danger Warning
- 19 Civil Emergency Message
- 20 Coastal Flood Watch
- 21 Coastal Flood Warning
- 22 Practice/Demo Warning
- 23 Dust Storm Warning
- 24 Earthquake Warning
- 25 Evacuation Immediate
- 26 Flash Flood Statement
- 27 Flash Flood Watch
- 28 Flash Flood Warning
- 29 Flood Statement
- 30 Flood Watch
- 31 Flood Warning
- 32 Fire Warning
- 33 Hazardous Materials Warning
- 34 Hurricane Statement
- 35 Hurricane Watch
- 36 Hurricane Warning
- 37 High Wind Watch
- 38 High Wind Warning
- 39 Local Area Emergency
- 40 Law Enforcement Warning
- 41 National Information Center Message
- 42 Network Message Notification
- 43 National Periodic Test
- 44 Nuclear Power Plant Warning
- 45 Special Marine Warning
- 46 Special Weather Statement
- 47 Shelter in Place Warning
- 48 Severe Thunderstorm Watch
- 49 Severe Thunderstorm Warning
- 50 Severe Weather Statement
- 51 911 Telephone Outage Emergency
- 52 Tornado Watch
- 53 Tornado Warning
- 54 Tropical Storm Watch
- 55 Tropical Storm Warning
- 56 Tsunami Watch
- 57 Tsunami Warning
- 58 Volcano Warning
- 59 Winter Storm Watch
- 60 Winter Storm Warning

Audio Option (third digit of the command)

You can optionally specify what type of audio is used for the message by entering a third digit in the command. This parameter is optional. If it's not included the message will default to using audio recorded from the Telephone.

- 0 Record audio from the Telephone (default, used if audio option is not specified)
- 1 Use the pre-recorded default user audio message
- 2 Use text-to-speech

Duration Option (fourth digit of the command)

You can optionally specify the duration of the EAS message. This parameter is optional. If it's not included the message will default to using a 15 minute duration.

- 0 15 minute duration (Default, used if the duration option is not specified)
- 1-9 the duration in hours (1 sets the duration to 1 hour, 9 sets a 9 hour duration)

Example: Activate RWT with 15 minute duration

To activate a Required Weekly Test message with a 15 minute duration, enter **12** followed by the **#** key.

- Enter **12** followed by the **#** key
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

Example: Activate RMT with audio from Telephone and 15 minute duration

To activate a Required Monthly Test message with a 15 minute duration and audio recorded from the Telephone, enter **11** followed by the **#** key.

- Enter **11** followed by the **#** key
  - The first two digits (**11**) activates an RMT message
  - The audio option (third digit) is omitted so the default is used (Telephone audio)
  - The duration option (fourth digit) is omitted so the default is used (15 minutes)
- Wait until the **BEEP** prompt is heard, recording starts immediately after the prompt
  - A **NACK** prompt is heard if the operation failed (because a message is in progress)
- Record the audio message by speaking into the Telephone (2 minutes maximum)
- Press the **#** key to stop recording audio
  - Press the * key to cancel the message activation and delete the audio
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

Example: Activate FLA with text-to-speech audio and a 1 hour duration

To activate a Flood Watch message with text-to-speech audio and a 1 hour duration, enter **3021** followed by the **#** key.

- Enter **3021** followed by the **#** key
  - The first two digits (**30**) activates a Flood Watch (FLA) message
  - The third digit (**2**) selects text-to-speech audio
  - The fourth digit (**1**) selects a 1 hour duration
- Wait until the **ACK** prompt is heard, message playback will begin after the prompt

THIS PAGE INTENTIONALLY LEFT BLANK

Specifications

General Specifications

EAS Encoder/Decoder compliant with all requirements defined in Part 11 of the FCC rules.

Operating Temperature: 0 to +50 C

Max. Operating Humidity: 95%

Supply Voltage: 117 VAC +/- 15%

Processor and Memory

Dual Core Processor, 2GB RAM, 40GB SATA SSD drive (minimum)

Chassis

2U RU chassis with 3.5” 320x240 color touch-screen LCD and speaker on the Front Panel

Communications

(2) RS-232 serial ports available on male DB-9 connectors

(4) USB ports

(2) 10/100/1000 Ethernet ports available on USB/RJ45 combo jacks

Audio

(6) Balanced 600 Ohm audio inputs for EAS monitoring each input can be configured for external audio or an optional internal radio receiver

- Economy models only support 4 audio inputs

(1) Line input and (1) line output

(2) Balanced analog audio outputs, 600 Ohm

(1) Balanced stereo analog audio switch, 600 Ohm

Video

NTSC video character generator

RS-170A color analog video (source only, does not overlay onto video)

Analog video switch with video bypass for fail-safe operation

General Purpose Inputs and Outputs

(6) General purpose outputs: isolated relay, maximum rating of 0.3 A @ 120 VAC or 1A @ 30 VDC

(2) TTL outputs: each TTL output can drive 2 TTL loads

(4) General purpose inputs: optically isolated dry contact closure inputs

Radio Receivers

(2) Radio receiver boards can be installed into the EASyCAP®

- Economy models only support 1 radio board

(3) Radio receivers are installed per board, each can be configured as AM, FM, or NOAA

AES-EBU Digital Audio Board (Optional Expansion Card)

(2) AES-EBU digital audio switches: each switch provides a pair of channels, 110 Ohm XLR

Alert audio automatically locks to the incoming bit rate and sample rate (up to 192 KHz)

Configurable as a switch or an audio source

Communications Expansion Board with RS-485 (Optional Card)

(1) 10/100 BaseT Ethernet ports

(1) Telephone port

(1) RS-485 serial port

Communication Board with 2 Ethernet ports (Optional Card)

(2) 10/100 BaseT Ethernet ports

(1) Telephone port

PCI-Express Expansion (Optional Expansion Card)

(1) PCI-Express card can be installed to provide additional capabilities such as SDI video, MPEG-2, MPEG-4, audio, video, or other capabilities.

Supports 1-lane and 4-lane PCI-Express cards and 16-lane PEG cards.

Supported PCI-Express cards must be purchased from Trilithic.

Trilithic EAS 2-Year Limited Warranty

Trilithic, Inc. ("Trilithic") warrants to the buyer that the product will be free from defects in materials and workmanship, under normal use, operating conditions and service for a period of two (2) years from date of delivery. Trilithic reserves the right, before having any obligation under this limited warranty, to inspect the damaged product, and all costs of shipping the product to Trilithic for inspection shall be borne solely by the buyer. Trilithic's obligation under this limited warranty shall be limited, at Trilithic's sole option, to replacing or repairing the product, or to replacing or repairing any defective part, F.O.B. Indianapolis, Indiana. If neither of the two options is reasonably available, then Trilithic, in its sole discretion, may provide a prorated refund to the buyer of the purchase price of the product, as evidenced by the proof of purchase, less any applicable service fees in accordance with the following schedule: months 0-3 = 100%; months 4-12 = 50%; and months 13–24 = 25%. Batteries and fans are not included or covered by this limited warranty. Any product or part that is repaired or replaced under this limited warranty shall be covered only for the remainder of the original warranty period which applied to the original product or part, or for ninety (90) days, whichever is longer. All products or parts that are exchanged for replacement shall become the property of Trilithic.

In order to recover under this limited warranty, buyer must make a written claim to Trilithic within sixty (60) days of the occurrence and must present acceptable proof of original ownership of the product (such as an original receipt, purchase order or similar documentation). In order for this limited warranty to be effective, the product must have been handled and used as set forth in the documentation accompanying the product and/or its packaging. This limited warranty shall not apply to any damage due to accident, misuse, abuse, neglect, fire or other casualty. Further, this limited warranty shall not apply to any product which has been altered or where the damage was caused by a part not supplied by Trilithic. Trilithic retains the final decision whether a product is within warranty conditions.

THE REMEDY SET FORTH HEREIN SHALL BE THE ONLY REMEDY AVAILABLE TO THE BUYER AND TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT SHALL TRILITHIC BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO, LOST REVENUES, LOST PROFITS, LOSS OF USE OF SOFTWARE, LOSS OR RECOVERY OF DATA, DOWNTIME, REPLACEMENT EQUIPMENT AND ANY THIRD PARTY CLAIMS ARISING OUT OF ANY THEORY OF RECOVERY INCLUDING WARRANTY, CONTRACT, STATUTORY OR TORT IN CONNECTION WITH THE PRODUCT, EVEN IF TRILITHIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING THE FOREGOING, IN THE EVENT THAT THIS LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT SHALL TRILITHIC'S ENTIRE LIABILITY TO BUYER EXCEED THE PURCHASE PRICE OF THE DEFECTIVE PRODUCT.

EXCEPT FOR THE LIMITED WARRANTY PROVIDED HEREIN, TO THE FULLEST EXTENT PERMITTED BY LAW, TRILITHIC DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE), WITH RESPECT TO THE PRODUCT OR ITS SUITABILITY FOR ANY USE INTENDED FOR IT BY THE BUYER. TO THE EXTENT ANY IMPLIED WARRANTIES MAY NONETHELESS EXIST BY OPERATION OF LAW, ANY SUCH WARRANTIES ARE LIMITED TO THE DURATION OF THIS LIMITED WARRANTY.

This limited warranty is non-transferable. This limited warranty does not affect any other legal rights buyer may have by operation of law. No agent, reseller, distributor or business partner of Trilithic is authorized to modify the terms of this limited warranty on behalf of Trilithic.

THIS PAGE INTENTIONALLY LEFT BLANK

TRILITHIC

9710 Park Davis Drive
Indianapolis, IN 46235
(317) 895-3600
www.trilithic.com

P/N 0010340001 04/15 Made in U.S.A.